Dated: 23 September 2013

Smart Energy Code

Contents

Version Control

Consolidated Version Number	Effective Date	Reason for Change	Overview of Modifications incorporated
1.0	23 September 2013	Designation by The Secretary of State pursuant to section 88(1) of the Energy Act 2008	First Publication
2.0	31 March 2014	Modifications to SEC version 1.0 as directed by the Secretary of State pursuant to section 88(1) of the Energy Act 2008	Communications Hub Financing Provisions
2.1	6 April 2014	Modifications to SEC version 2.0 as directed by the Secretary of State pursuant to section 88(1) of the Energy Act 2008	SEC2 amendments to sections of SEC already in force
2.2	27 May 2014	Modification to SEC version 2.1 as directed by the SEC Panel pursuant to SECMP 0001	Updating the SEC to reflect abolition of the National Consumer Council
3.0	31 July 2014	Modifications to SEC version 2.2 as directed by the Secretary of State pursuant to section 88(1) of the Energy Act 2008	Smart Metering System Requirements, Testing Service, Smart Metering Key Infrastructure and Appendices, Testing During Transition and SEC3 amendments to sections already in force
4.0	14 January 2015	Modifications to SEC version 3.0 as directed by the Secretary of State pursuant to Section 88(1) of the Energy Act 2008	Security Governance, Assurance and Privacy, Communications Hubs, Enrolment and Adoption of SMETS1 meters and SEC4.0 amendments to sections already in force
4.1	26 January 2015	Modifications to SEC version 4.0 as directed by the Secretary of State in accordance with SEC Section X3.1, SEC Section X5.4 and Condition 22 of the DCC Licence	Activation of Section H15, designation of the DCC Gateway Connection Code of Connection as a Subsidiary Document and consequential changes to sections already in force
4.2	18 March 2015	Modifications to SEC version 4.1 as directed by the Secretary of State pursuant to Section	Party and RDP Signifiers, Party, User and RDP Identifiers and SEC4.2 amendments to sections already in force

		88(1) of the Energy Act 2008	
4.3	1 July 2015	Modifications to SEC version 4.2 as directed by the Secretary of State pursuant to Section 88(1) of the Energy Act 2008	SEC Schedule 7 providing a Specimen Enabling Agreement, DCC Services and SEC4.3 amendments to sections already in force
4.4	14 September 2015	Modifications to SEC version 4.3 as directed by the Secretary of State in accordance with SEC Section X5.4 and Condition 22 of the DCC Licence	Designation of the CH Handover Support Materials as a Subsidiary Document and consequential changes to sections already in force.
4.5	28 September 2015	Modifications to SEC version 4.4 as directed by the Secretary of State in accordance with SEC Section X5.4 and Condition 22 of the DCC Licence	Designation of the Enduring Testing Approach Document as a Subsidiary Document and consequential changes to sections already in force.
4.6	21 October 2015	Modifications to SEC version 4.5 as directed by the Secretary of State in accordance with SEC Section X5.4 and Condition 22 of the DCC Licence	Designation of the SMKI and Repository Test Scenarios Document and Subsidiary Document and consequential changes to sections already in force.
4.7	9 February 2016	Modifications to SEC version 4.6 as directed by the Secretary of State in accordance with SEC Section X5.4 and Condition 22 of the DCC Licence	Designation of the SMKI Registration Authority Policies and Procedure (SMKI RAPP) and SMKI Recovery Procedure and consequential changes to sections already in force.
4.8	10 February 2016	Modifications to SEC version 4.7 as directed by the Secretary of State pursuant to Section 88(1) of the Energy Act 2008 Modifications to SEC version 4.6 as directed by the Secretary of State in accordance with SEC	Designation of further Communications Hub provisions. Designation of SMKI and DCC Key Infrastructure provisions. Designation of the CH Installation and Maintenance Support Materials (CHIMSM) and consequential changes to sections already in force.

		Section X5.4 and Condition 22 of the DCC Licence	
4.9	9 March 2016	Modifications to SEC version 4.8 as directed by the Secretary of State in accordance with SEC Section X5.4 and Condition 22 of the DCC Licence	Designation of SMKI Interface Design Specification, SMKI Code of Connection, SMKI Repository Interface Design Specification, SMKI Repository Code of Connection, IKI Certificate Policy and the Common Test Scenarios Document. Re-Designation of the DCC Gateway Connection Code of Connection and consequential changes to sections already in force.
4.10	18 April 2016	Modifications to SEC version 4.9 as directed by the Secretary of State in accordance with SEC Section X6	Designation of provisions for Interim Device and User Testing (Section X9).
4.11	6 June 2016	Modifications to SEC version 4.10 as directed by the Secretary of State pursuant to SEC Section X3.1, X5 and Condition 22.27 of the DCC Licence	Activation of Sections H1, H2 and H3.22 Designation of the DCCKI Certificate Policy and DCCKI Registration Authority Policies and Procedures
4.12	15 June 2016	Modifications to SEC version 4.11 as directed by the Secretary of State pursuant to Section 88(1) of the Energy Act 2008	Amendments to sections of SEC already in force
4.13	6 July 2016	Modifications to SEC version 4.12 as directed by the Secretary of State pursuant to SEC Section X3.1, X5, X6 and Condition 22 of the DCC Licence	Designation of Registration Data Interface Specification and Registration Data Interface Code of Connection. Re-designation of the SMKI Registration Authority Policies and Procedures, and the IKI Certificate Policy.
4.14	13 July 2016	Modifications to SEC version 4.13 as directed by the Secretary of State pursuant to Section 88 (1) and 89 of the Energy	Designation of SEC Section Z - Alt HAN Arrangements. Designation of Appendix T -DCCKI Interface Design Specification,

		Act 2008, and pursuant to SEC Sections X3.1, X5, and X6	Appendix U- DCCKI Repository Interface Design Specification, and Appendix V - DCCKI CoCo and DCCKI Repository CoCo. SEC Appendices A, B and C deleted and re-designated.Amendments to SEC sections already in force.
4.15	18 August 2016	Modifications to SEC version 4.14 as directed by the Secretary of State pursuant to Section 88 (1) and 89 of the Energy Act 2008, and pursuant to SEC Appendix J. Modification to SEC version 4.14 as directed by the SEC Panel pursuant to SECMP0017 with effect 17 August 2016.	Re-designation of an updated version of SEC Appendix J – Enduring Testing Approach Document. Amendments to SEC Section D6.3 to D6.4.
4.16	20 October 2016	Modification to SEC version 4.15 as directed by the Secretary of State pursuant to Section X5 and Condition 22 of the DCC Licence.	Re-designation of SEC Appendix R: Common Test Scenarios Document.
4.17	27 October 2016	Modification to SEC version 4.16 as directed by the Secretary of State pursuant to Section 88 (1) and 89 of the Energy Act 2008, and pursuant to SEC Appendix Z.	Designation of SEC Appendix Z: CPL Requirement Document. Activation of SEC Section F2.
5.0	8 November 2016	Modification to SEC version 4.17 as directed by the Secretary of State pursuant to Section 88 (1) and 89 of the Energy Act 2008. Activation of multiple SEC Sections, re-designation, and incorporation of new	Activation of SEC Sections: • F3 (Panel Dispute Resolution Role) • F4.9 (Power Outage Alerts) • H3 (DCC User Interface), but excluding H3.27 • H4 (Processing Service Requests) • H5 (Smart Metering Inventory & Enrolment Services)

		Subsidiary Documents necessary for DCC Live.	• H6 (Decommissioning, Withdrawal & Suspension of Devices) • H8 (Service Management, SSI & Service Desk); • H9 (Incident Management Policy) • H10.9-H10.13 (Business Continuity) • H11 (Parse and Correlate) • H14.36 (DCC Internal System Change Testing Designation of new SEC Schedules: • Schedule 8 GB Companion Specification • Schedule 9 Smart Metering Equipment Technical Specifications • Schedule 10 Communications Hub Technical Specifications Designation of new SEC Appendices • Appendix AA - Threshold Anomaly Detection Procedures • Appendix AB - Service Request Processing Document • Appendix AC - Inventory, Enrolment and Withdrawal Procedures • Appendix AD - DCC User Interface Specification • Appendix AE - DCC User Interface Code of Connection • Appendix AF - Message Mapping Catalogue • Appendix AG - Incident Management Policy • Appendix AH - Self-Service Interface Design Specification • Appendix AI - Self-Service Interface Code of Connection

			Re-designation of SEC Appendices: • Appendix E - DCC User Interface Services Schedule • Appendix H - CH Handover Support Materials; • Appendix I - CH Installation and Maintenance Support Materials; • Appendix L - SMKI Recovery Procedure; • Appendix O - SMKI Repository Interface Design Specification; • Appendix G - DCC Gateway Connection Code of Connection; • Appendix K - SMKI and Repository Test Scenarios Document; • Appendix M - SMKI Interface Design Specification; • Appendix N - SMKI Code of Connection
5.1	14 December 2016	Implementation of two Modifications Proposals approved via Change Board vote on 23 November 2016.	Implementation of Modification Proposals: • Amendment to Section L due to SECMP0022 “Expanding SMKI PMA membership and removing Alternate restrictions” • Amendments to Schedule 5 due to SECMP0020 “Removal of the confidential classification of the unique identifiers listed in SEC Schedule 5”
5.2	21 December 2016	Modification to SEC version 5.1 as directed by the Secretary of State pursuant to Section 88 (1) and 89 of the Energy Act 2008.	Redesignation of Appendix AC – Inventory, Enrolment and Withdrawal Procedures

5.3	26 January 2017	Modification to SEC version 5.2 as directed by the Secretary of State pursuant to section 88(1) of the Energy Act 2008.	Amendments to Section N: SMETS1 Meters, including the designation of a new Section N4A
5.4	9 February 2017	Modifications to SEC version 5.3 as directed by the Secretary of State pursuant to section 89 of the Energy Act 2008. Modifications as directed by the Secretary of State pursuant to SEC Section X5.	Amendments in relation to testing including: testing required to implement changes to the SEC; Enduring Registration Data Provider Entry Process Testing; changes to the Enduring Testing Approach Document (ETAD); provision of variant Communications Hubs for testing. Other Changes include amendments to the Ofgem Significant Code Review process; Privacy requirements; making certain transitional variations enduring; the definition of RDP Systems; changes to accommodate multiple versions of Technical Specifications and multiple versions of DUIS and other minor miscellaneous changes. The Secretary of State direction designates Schedule 11 and Smart Metering Equipment Technical Specifications Version 1.2.
5.5	15 March 2017	Implementation of a Modification Proposal approved via Change Board vote on 22 February 2017.	Amendment to Section G due to implementation of SECMP0026 “Changes to the Security Sub-Committee Nomination Process”.
5.6	1 April 2017	Implementation of a Modification Proposal approved by the Authority on 17 January 2017.	Amendments to Sections A and J due to implementation of SECMP0016 “Consideration of “maximum credit value” in credit cover calculation”.
5.7	11 May 2017	Implementation of a Modification Proposal approved via Change Board vote on the 19 April 2017.	Amendments to Section A and Appendix H due to implementation of SECMP0033 “CH Handover Support Materials”.

5.8	13 July 2017	Implementation of a Modification Proposal approved via Change Board vote on the 21 June 2017.	Amendments to Appendix B and Appendix S due to implementation of SECMP0035 “Updates to SEC Appendix B – Organisation ARL expiration date to be aligned to DCCKI ARL”.
5.9	21 July 2017	Modifications to SEC version 5.8 as directed by the Secretary of State pursuant to section 89 of the Energy Act 2008.	Re-designation of Appendix AC – Inventory Enrolment and Withdrawal Procedures (version 1.2); and Appendix AD – DCC User Interface Specification (version 1.1).
5.10	14 September 2017	Implementation of a Modification Proposal approved via the Change Board on the 23 August 2017.	Amendments to Section H due to implementation of SECMP0036 “Single User ID for Users acting in one or more User Roles”.
5.11	6 November 2017	Modifications to SEC version 5.10 as directed by the Secretary of State pursuant to Section 88(1) of the Energy Act 2008	Amendments to Appendix AH, Schedule 8 and Schedule 11 as directed by the Secretary of State.
5.12	22 November 2017	Implementation of a Modification Proposal approved via the Change Board on 25 October 2017.	Amendments to Section G due to implementation of SECMP0040 “Changes to how DCC Users schedule and carry out User Security Assessments after completion of the User Entry Process”.
5.13	1 February 2018	Modifications to SEC version 5.12 as directed by the Secretary of State pursuant to section 89 of the Energy Act 2008.	Amendments to Appendix H, Appendix I, Schedule 9 – SMETS1 v1.2, Schedule 9 – SMETS2 v2.0 and Schedule 11 – TS Applicability Tables. Designation of new SEC Schedules and Appendices to sit alongside existing versions: • Schedule 8 – GBCS v2.0 • Schedule 8 – GBCS v3.0 • Schedule 9 – SMETS2 v3.0 • Schedule 9 – SMETS2 v4.0 • Schedule 10 – CHTS v1.1 • Schedule 10 – CHTS v1.2

			• Appendix AD – DUIS v2.0 • Appendix AF – MMC v2.0
5.14	22 February 2018	Modifications to SEC version 5.13 as directed by the Secretary of State pursuant to Section 88(1) of the Energy Act 2008 Modifications to SEC version 5.13 as directed by the Secretary of State pursuant to SEC Section X5	Amendments to SEC Section A Designation of Appendix AJ – SEC Variation Testing Approach Document
5.15	25 May 2018	Implementation of a Modification Proposal approved by the Authority on 1 May 2018.	Amendments to Section A, Section I, Section M and Appendix AG due to implementation of SECMP0045 "Incorporation of the requirements of the General Data Protection Regulations".
5.16	31 May 2018	Modifications to SEC version 5.15 as directed by the Secretary of State pursuant to Section 88(1) of the Energy Act 2008	Designation of Section P – Production Proving; and amendments to Section A, Section C, Section E, Section F, Section H, Section J, Section K, Section L and Section X as directed by the Secretary of State.
5.17	5 June 2018	Modifications to SEC version 5.16 as directed by the Secretary of State pursuant to SEC Section X5	Amendments to Schedule 8 – GBCS v3.0, Schedule 11 – TS Applicability Tables and Appendix AD – DUIS v2.0 Designation of new SEC Schedule 8 – GBCS v2.1 and SEC Schedule 8 – GBCS v3.1 to sit alongside existing versions.
5.18	8 June 2018	Modifications to SEC version 5.17 as directed by the Secretary of State pursuant to SEC Section X5. Modifications to SEC version 5.17 as directed by the Secretary of State pursuant to SEC Section X5.	Amendments to Appendix J – Enduring Test Approach Document and Appendix R – Common Test Scenarios Document. Amendments to Appendix B – Organisation Certificate Policy and Appendix M – SMKI Interface Design Specification.

5.19	25 June 2018	Modifications to SEC version 5.18 as directed by the Secretary of State pursuant to SEC Section X5.	Amendments to Appendix AJ – SEC Variation Testing Approach Document.
5.20	18 July 2018	Modifications to SEC version 5.19 as directed by the Secretary of State pursuant to Section 88(1) of the Energy Act 2008.	Amendments to Section A, Section B, Section C, Section F, Section G, Section H, Section I, Section L, Section N, Section T, Section X, Section Z and Schedule 7
5.21	22 July 2018	Implementation of a Modification Proposal approved via Change Board vote on 22 July 2018.	Amendments to Section A and Section G due to implementation of SECMP0044 "User Security Assessment of a Shared Resource".
5.22	18 September 2018	Modifications to SEC version 5.21 as directed by the Secretary of State pursuant to SEC Section X5.	Amendments to Section A and designation of Appendix AK – SEC Variation Testing Approach Document for SMETS1 Services.
5.23	4 October 2018	Modifications to SEC version 5.22 as directed by the Secretary of State pursuant to SEC Section X5.	Amendments to TS Applicability Tables.
6.0	28 October 2018	Modifications to SEC version 5.23 as directed by the Secretary of State pursuant to SEC Section X5.	Amendments to SEC Appendix AB – Service Request Processing Document and SEC Appendix E – DCC User Interface Services Schedule and consequential changes to SEC Section A – Definitions and Interpretation and SEC Schedule 11 – TS Applicability Tables.
6.1	1 November 2018	Implementation of Modification Proposals approved by the Authority or by Change Board vote.	Amendments to SEC Section A, Section D, Section F, Section G, Section H, Section J, Section M, Section X, Appendix E, Appendix S, Appendix W, Appendix AA, Appendix AD and Appendix AH, due to the implementation of Modification Proposals SECMP0008, SECMP0019, SECMP0027, SECMP0029, SECMP0034, SECMP0047,

			SECMP0050, SECMP0051 and SECMP0052
6.2	8 November 2018	Implementation of Modification Proposals approved by the Authority or by Change Board vote	Amendments to Section G, Schedule 9 and Schedule 11 due to the implementation of Modification Proposals SECMP0006, SECMP0048 and SECMP0065.
6.3	5 December 2018	Modifications to SEC version 6.2 as directed by the Secretary of State pursuant to SEC Section X5.	Amendments to SEC Schedule 11 – TS Applicability Tables.
6.4	21 January 2019	Re-designation of an amended version of the Inventory Enrolment and Decommissioning Procedures Document (IEDP) as directed by the Secretary of State pursuant to SEC Section X5.	Amendments and re-designation of Appendix AC
6.5	28 January 2019	Implementation of Modification Proposal approved by the Authority.	Amendments to SEC Section M and Section Z, due to the implementation of Modification Proposal SECMP0068
6.6	14 February 2019	Modifications to SEC version 6.5 as directed by the Secretary of State pursuant to SEC Section X5.	Designation of Appendix AL – SMETS1 Transition and Migration Approach Document
6.7	28 February 2019	Implementation of Modification Proposals approved by the Authority or by Change Board vote.	Amendments to SEC Section A, Section D, Section F, Section G and Section Z, due to the implementation of Modification Proposals SECMP0009, SECMP0057, SECMP0059, SECMP0061 and SECMP0064. Corrections to Section L.
6.8	4 March 2019	Implementation of Modification Proposal approved by the Authority.	Amendments to SEC Section A, Section C, Section D, Section F, Section G, Section L, Section M, Section Z and Appendix AG, due to the implementation of Modification Proposal SECMP0049.

6.9	13 March 2019	Modifications to SEC version 6.8 as directed by the Secretary of State pursuant to SEC Section X5.	Re-designation of SEC Section A, Section F, Section G, Section H, Section I, Section L, Section N, Section P, Appendix J, Appendix R and Appendix Z.
6.10	15 April 2019	Re-designation of an amended version of the Common Test Scenarios Document (CTSD) as directed by the Secretary of State pursuant to SEC Section X5.	Amendments and re-designation of Appendix R.
6.11	23 April 2019	Implementation of Modification Proposal approved by the Authority.	Amendments to SEC Section A, Section H and Section M, due to the implementation of Modification Proposal SECMP0043.
6.12	26 April 2019	Implementation of Modification Proposal approved by the Change Board.	Amendments to SEC Section Z, due to the implementation of Modification Proposal SECMP0070.
6.13	14 June 2019	Re-designation of an amended version of the SEC Variation Testing Approach Document for SMETS1 Services (SVTAD) as directed by the Secretary of State pursuant to SEC Section X5.	Amendments and re-designation of Appendix AK.
6.14	21 June 2019	Re-designation of an amended version of the SMETS1 Transition and Migration Approach Document as directed by the Secretary of State pursuant to SEC Section X5.	Amendments and re-designation of Appendix AL.
6.15	27 June 2019	Implementation of Modification Proposal approved by the Change Board.	Amendments to SEC Section A, Section H, Appendix I, Appendix T, Appendix W, Appendix AA, Appendix AH and Appendix AI due to the implementation of Modification Proposal SECMP0058.
6.16	4 July 2019	Modifications to SEC version 6.15 as directed	Designation of SEC Schedule 8 Version 3.2, Schedule 9 Version

		by the Secretary of State pursuant to SEC Section X5 and for Modification Proposals approved by the Authority or by Change Board vote. Modifications to SEC version 6.15 as directed by the Secretary of State pursuant to Section 88(1) of the Energy Act 2008	4.2 and Schedule 10 Version 1.3 and re-designation of SEC Schedule 8 Version 3.1, Schedule 9 Version 4.0, Schedule 9 Version 4.1, Schedule 10 Version 1.2 and Schedule 11 as directed by the Secretary of State and for Modification Proposals SECMP0018, SECMP0023, SECMP0025 and SECMP0055. Amendments to SEC Section A, Section F and Section G.
6.17	28 July 2019	Modifications to SEC version 6.16 as directed by the Secretary of State pursuant to SEC Section X5.	Designation of SEC Appendix AD – DUIS v3.0, Appendix AF – MMC v3.0 and Appendix AM 'SMETS1 Supporting Requirements'. Amendments to SEC Appendix E, Appendix I, Appendix AA, Appendix AB, Appendix AC, Appendix AH and Appendix AL. Corrections to SEC Section A.
6.18	18 October 2019	Re-designation of an amended version of the SEC Technical Specification Applicability Tables (TSAT) as directed by the Secretary of State pursuant to SEC Section X5.	Amendments to SEC Schedule 11 – TS Applicability Tables.
6.19	25 October 2019	Modification to SEC Appendix AK as directed by the DCC pursuant to Clause 4.2 of the SEC Variation Testing Approach Document for SMETS1 Services (SMETS1 SVTAD).	Amendments to SEC Appendix AK 'SEC Variation Testing Approach Document for SMETS1 Services'.
6.20	4 November 2019	Modifications to SEC version 6.19 as directed by the Secretary of State	Amendments to SEC Section G. Amendments to SEC Schedule 11

		pursuant to SEC Section X5 and for Modification Proposals approved by the Authority or by Change Board vote.	– TS Applicability Tables. Amendments to SEC Appendix AK 'SEC Variation Testing Approach Document for SMETS1 Services'.
6.21	29 November 2019	November 2019 SEC Release. Implementation of Modification Proposals approved by the Change Board and the Authority.	Amendments to SEC Section J, Section K, and Section L. Amendments to SEC Appendix D, Appendix E, Appendix K, Appendix M, Appendix N, Appendix Q, Appendix AC, Appendix AD, and Appendix AF. These are due to the implementation of Modification Proposals SECMP0018, SECMP0023, SECMP0025, SECMP0039, SECMP0055, SECMP0060, MP071, MP073, MP074 and MP076.
6.22	13 December 2019	Modifications to SEC version 6.21 as directed by the Secretary of State pursuant to SEC Section X5.	Amendments to SEC Appendix J 'Enduring Testing Approach Document' and Appendix AM 'SMETS1 Supporting Requirements'.
6.23	20 January 2020	Implementation of a Modification Proposal approved by the Change Board.	Amendments to SEC Appendix R 'Common Testing Scenarios Document' due to the implementation of MP089.
6.24	31 January 2020	Implementation of a Modification Proposal approved by the Change Board.	Amendments to SEC Section A 'Definitions and Interpretation', Section D 'Modification Process' and Section I 'Data Privacy' due to the implementation of SECMP0069.
6.25	6 February 2020	Modification to SEC Appendix AK as directed by the DCC pursuant to Clause 4.2 of the SEC Variation Testing Approach Document for SMETS1 Services.	Amendments to SEC Appendix AK 'SEC Variation Testing Approach Document for SMETS1 Services'.
7.0	27 February 2020	February 2020 SEC Release.	Amendments to SEC Section G, Section Z and Appendix H.

		Implementation of Modification Proposals approved by the Change Board and the Authority.	These are due to the implementation of Modification Proposals MP086, MP091 and MP097.
8.0	13 March 2020	Modification to the SEC as directed by the Secretary of State pursuant to SEC Section X5.	Amendments to SEC Appendix AL 'SMETS1 Transition and Migration Approach Document'.
9.0	16 March 2020	Modifications to the SEC as directed by the Secretary of State pursuant to Section 88(1) of the Energy Act 2008.	Amendments to SEC Section A, Section G, Section H, Section I, Section K, Section L and Section X.
10.0	3 April 2020	Modification to SEC Appendix AK as directed by the DCC pursuant to Clause 4.2 of the SEC Variation Testing Approach Document for SMETS1 Services.	Amendments to SEC Appendix AK 'SEC Variation Testing Approach Document for SMETS1 Services'.
11.0	6 May 2020	June 2020 SEC Release. Implementation of Modification Proposals approved by the Change Board. Modification to the SEC as directed by the Secretary of State pursuant to Section X5 and Condition 22 of the DCC Licence.	The June 2020 SEC Release makes amendments to SEC Section H, Appendix E and Appendix AB. These are due to the implementation of Modification Proposals SECMP0053 and SECMP0062 (Part 1). The Secretary of State modification to the SEC makes amendments to SEC Appendix AL and Appendix AM.
12.0	7 May 2020	June 2020 SEC Release Implementation of a Modification Proposal approved by the Change Board.	Amendments to SEC Section Z. These are due to the implementation of Modification Proposal MP114.
13.0	27 May 2020	Implementation of a Modification Proposal approved by the Authority.	Amendments to SEC Section F due to the implementation of Modification Proposal MP130.
14.0	29 May 2020	Implementation of a Modification Proposal	Amendments to SEC Schedule 11 'TS Applicability Tables' due to the

		approved by the Change Board.	implementation of Modification Proposal MP123.
15.0	11 June 2020	Modifications to the SEC as directed by the Secretary of State pursuant to Section 88(1) of the Energy Act 2008.	Amendments to SEC Section A, Section E, Section G, Section K, and Section L.
16.0	15 June 2020	Modification to the SEC as directed by the Secretary of State pursuant to SEC Section X5.	Amendments to SEC Appendix AL 'SMETS1 Transition and Migration Approach Document'.
17.0	1 July 2020	Modification to the SEC as directed by the Secretary of State pursuant to SEC Section X5.	Designation of Appendix AN 'SEC Variation Testing Approach Document for BEIS Changes included in the November 2020 SEC Release'. Amendments to SEC Section A 'Definitions and Interpretation'.
18.0	23 July 2020	Implementation of a Modification Proposal approved by the Change Board.	Amendments to SEC Section G 'Security' due to the implementation of Modification Proposal MP135.
19.0	26 July 2020	Modification to the SEC as directed by the Secretary of State pursuant to Section X5 and Condition 22 of the DCC Licence.	Amendments to SEC Appendix AL and Appendix AM.
20.0	31 July 2020	Modification to the SEC as directed by the Secretary of State pursuant to Section X5 and Condition 22 of the DCC Licence.	Amendments to SEC Appendix AG 'Incident Management Policy'.
21.0	18 September 2020	Modifications to the SEC as directed by the Secretary of State pursuant to Section X5 and Condition 22 of the DCC Licence, and Section 88(1) of the Energy Act 2008.	Amendments to SEC Section A, Section F, Section G, Section H, Section K, Section L, Section N, Section T, Section X, Section Z, Schedule 11, Appendix L and Appendix AL. Implementation of Device Level Versioning to SEC Schedule 9: • 'Smart Metering

			Equipment Technical Specifications 1' 1 Feb 2018 - 'Smart Metering Equipment Technical Specifications 2' 1 Feb 2018 - 'Smart Metering Equipment Technical Specifications 2' 8 Nov 2018 - 'Smart Metering Equipment Technical Specifications 2' 4 Jul 2019 Designation of SEC Appendix AO and Appendix AP.
22.0	25 September 2020	Modification to the SEC as directed by the Secretary of State pursuant to Section X5 and Condition 22 of the DCC Licence.	Amendments to SEC Appendix AK 'SEC Variation Testing Approach Document for SMETS1 Services'
23.0	7 October 2020	Modification to the SEC as directed by the Secretary of State pursuant to Section X5 and Condition 22 of the DCC Licence.	Amendments to SEC Appendix J, Appendix R and Appendix AK.
24.0	6 November 2020	Modification to SEC Appendix AK as directed by the DCC pursuant to Clause 4.2 of the SEC Variation Testing Approach Document for SMETS1 Services.	Amendments to SEC Appendix AK 'SEC Variation Testing Approach Document for SMETS1Services'.
25.0	12 November 2020	Modification to the SEC as directed by the Secretary of State pursuant to Section X5 and Condition 22 of the DCC Licence.	Amendments to SEC Appendix AL 'SMETS1 Transition and Migration Approach Document'.
26.0	24 November 2020	Modification to the SEC as directed by the Secretary of State pursuant to Section X5	Amendments to: - SEC Appendix AB 'Service Request Processing Document' - SEC Appendix AD 'DCC

		and Condition 22 of the DCC Licence.	User Interface Specification' v3.0 • SEC Appendix AD 'DCC User Interface Specification' v3.1 • SEC Appendix AM 'SMETS1 Supporting Requirements'
27.0	29 November 2020	November 2020 SEC Release Modification to the SEC as directed by the Secretary of State pursuant to SEC Section X3.1, X5 and Condition 22 of the DCC Licence. Implementation of Modification Proposals approved by the Change Board and the Authority.	Amendments to: • Section A • Section G • Section I • Section J • Section L • Schedule 11 • Appendix A • Appendix B • Appendix D • Appendix E • Appendix I • Appendix L • Appendix M • Appendix O • Appendix Q • Appendix AB • Appendix AC Implementation of: • Schedule 8 ‘GB Companion Specification’ v4.0 • Schedule 9 ‘Smart Metering Equipment Technical Specifications 2' - 29 November 2020 • Schedule 10 'Communications Hub Technical Specifications' v1.4 • Appendix AD ‘DCC User Interface Specification’ v4.0 • Appendix AF ‘Message Mapping Catalogue’ v4.0
28.0	4 December 2020	Modification to the SEC as directed by the Secretary of State pursuant to Section X5	Amendments to SEC Appendix AM 'SMETS1 Supporting Requirements'.

		and Condition 22 of the DCC Licence.	
29.0	21 December 2020	Modification to the SEC as directed by the Secretary of State pursuant to Section X5 and Condition 22 of the DCC Licence.	Amendments to SEC Appendix AL 'SMETS1 Transition and Migration Approach Document'.
30.0	13 January 2021	Modification to the SEC as directed by the Secretary of State pursuant to Section X5 and Condition 22 of the DCC Licence.	Amendments to SEC Appendix E 'DCC User Interface Services Schedule'.
31.0	21 January 2021	Implementation of a Modification Proposal approved by the Change Board.	Amendments to SEC Schedule 11 'TS Applicability Tables' due to the implementation of Modification Proposal MP139.
32.0	22 January 2021	Modifications to the SEC as directed by the Secretary of State pursuant to Section 88(1) of the Energy Act 2008.	Amendments to SEC Section A 'Definitions and Interpretation'.
33.0	25 January 2021	Implementation of a Modification Proposal approved by the Authority.	Amendments to SEC Section A 'Definitions and Interpretation' and to Section F 'Smart Metering System Requirements' due to the implementation of MP111.
34.0	25 February 2021	February 2021 SEC Release. Implementation of Modification Proposals approved by the Change Board and the Authority.	Amendments to SEC Section A, Section H and Appendix AL. These are due to the implementation of Modification Proposals MP092 and MP122A.
35.0	28 February 2021	Modification to the SEC as directed by the Secretary of State pursuant to Section X5 and Condition 22 of the DCC Licence.	Amendments to SEC Appendix AL and Appendix AM. Designation of SEC Appendix AP 'FOC S1SPKI Certificate Policy'.
36.0	30 March 2021	Modification to the SEC as directed by the Secretary of State pursuant to Section X5	Amendments to SEC Appendix AL and Appendix AM.

		and Condition 22 of the DCC Licence.	
37.0	23 April 2021	Implementation of a Modification Proposal approved by the Change Board.	Amendments to SEC Schedule 11 'TS Applicability Tables' due to the implementation of Modification Proposal MP148.
38.0	14 June 2021	Modification to the SEC as directed by the Secretary of State pursuant to Section X5 and Condition 22 of the DCC Licence.	Amendments to SEC Appendix AL 'SMETS1 Transition and Migration Approach Document'.
39.0	16 June 2021	Modification to the SEC as directed by the Secretary of State pursuant to Section X5 and Condition 22 of the DCC Licence.	Amendments to SEC Appendix M 'SMKI Interface Design Specification'.
40.0	24 June 2021	June 2021 SEC Release. Implementation of Modification Proposals approved by the Change Board and the Authority.	Amendments to SEC Section H, Section I, Section J, Appendix I, and Appendix O. These are due to the implementation of Modification Proposals MP106, MP144, MP146, MP147 and MP153. Amendments to SEC Appendix R due to the phased implementation of SECMP0007.
41.0	2 July 2021	Modification to the SEC as directed by the Secretary of State pursuant to Section X5 and Condition 22 of the DCC Licence.	Amendments to SEC Appendix AL 'SMETS1 Transition and Migration Approach Document'.
42.0	20 July 2021	Modification to the SEC as directed by the Secretary of State pursuant to Section X5 and Condition 22 of the DCC Licence.	Amendments to: • Section A 'Definitions and Interpretation' • Section H 'DCC Services' • Appendix Z 'CPL Requirements Document' • Appendix AD 'DCC User Interface Specification' v3.0, v3.1 and v4.0 • Appendix AL 'SMETS1 Transition and Migration

			Approach Document' • Appendix AM 'SMETS1 Supporting Requirements'
43.0	30 July 2021	Modification to the SEC as directed by the Secretary of State pursuant to Section X5 and Condition 22 of the DCC Licence.	Amendments to: • SEC Section A 'Definitions and Interpretation • SEC Appendix B 'Organisation Certificate Policy' Implementation of: • SEC Appendix AQ 'SEC Variation Testing Approach Document for the CH&N Arrangements' • SEC Appendix AR 'SEC Variation Testing Approach Document for the Enduring Change of Supplier Arrangements'
44.0	25 August 2021	Modification to the SEC as directed by the Secretary of State pursuant to Section X5 and Condition 22 of the DCC Licence.	Amendments to: • SEC Appendix AK 'SEC Variation Testing Approach Document for SMETS1 Services' • SEC Appendix AL 'SMETS1 Transition and Migration Approach Document'
45.0	1 September 2021	Implementation of a Modification Proposal approved by the Authority.	Amendments to: • SEC Section A 'Definitions and Interpretation' • SEC Section B ‘Accession’ • SEC Section D ‘Modification Process' • SEC Section E ‘Registration Data’ • SEC Section K ‘Charging Methodology’ • SEC Schedule 5 ‘Accession Information’ • SEC Appendix X ‘Registration Data Interface Specification’ • SEC Appendix Y ‘Registration Data Interface Code of Connection’

			These are due to the implementation of Modification Proposal MP161.
46.0	22 September 2021	Modification to SEC Appendix AK as directed by the DCC pursuant to Clause 4.2 of the SEC Variation Testing Approach Document for SMETS1 Services.	Amendments to SEC Appendix AK 'SEC Variation Testing Approach Document for SMETS1 Services'
47.0	4 October 2021	Implementation of a Modification Proposal approved by the Authority.	Amendments to: • SEC Section A 'Definitions and Interpretation' • SEC Section L 'Smart Metering Key Infrastructure and DCC Key Infrastructure' • SEC Section M 'General' • SEC Appendix B 'Organisation Certificate Policy' • SEC Appendix Q 'IKI Certificate Policy' • SEC Appendix S 'DCCKI Certificate Policy' These are due to the implementation of Modification Proposal MP134A.
48.0	8 October 2021	Modification to the SEC as directed by the Secretary of State pursuant to Section X5 and Condition 22 of the DCC Licence.	Amendments to: • SEC Section A 'Definitions and Interpretation' • SEC Appendix Z 'CPL Requirements Document' • SEC Appendix AM 'SMETS1 Supporting Requirements'
49.0	25 October 2021	Modification to the SEC as directed by the Secretary of State pursuant to Section 88(1) of the Energy Act 2008 and to Section X5 and Condition 22 of the DCC Licence.	Amendments to: • SEC Section A 'Definitions and Interpretation' • SEC Section G 'Security' • SEC Section L 'Smart Metering Key Infrastructure and DCC Key Infrastructure' Implementation of: • SEC Appendix AS

			'ECoS Transition and Migration Approach Document'
50.0	4 November 2021	November 2021 SEC Release Implementation of Modification Proposals approved by the Change Board and the Authority. Modification to the SEC as directed by the Secretary of State pursuant to Section X5 and Condition 22 of the DCC Licence.	Amendments to: • Section A • Section C • Section H • Section K • Schedule 7 • Schedule 11 • Appendix E • Appendix J • Appendix X • Appendix AB • Appendix AL • Appendix AM Implementation of: • Schedule 8 'GB Companion Specification' v4.1 • Schedule 9 'Smart Metering Equipment Technical Specifications 2' – 4 November 2021 • Schedule 10 'Communications Hub Technical Specifications' v1.5 • Appendix AD 'DCC User Interface Specification' v5.0 • Appendix AF 'Message Mapping Catalogue' v5.0
51.0	11 November 2021	Implementation of a Modification Proposal approved by the Change Board.	Amendments to: • SEC Section B 'Accession' • SEC Appendix AC 'Inventory, Enrolment and Decommissioning Procedures' These are due to the implementation of Modification Proposal MP128B.
52.0	17 November 2021	Implementation of a Modification Proposal approved by the Authority.	Amendments to: • SEC Section A 'Definitions and Interpretation' • SEC Section B 'Accession' • SEC Section L 'Smart

			Metering Key Infrastructure and DCC Key Infrastructure' These are due to the implementation of Modification Proposal MP185.
53.0	9 December 2021	Modification to the SEC as directed by the Secretary of State pursuant to Section X5 and Condition 22 of the DCC Licence.	Amendments to: • SEC Appendix AK 'SEC Variation Testing Approach Document for SMETS1 Services' • SEC Appendix AL 'SMETS1 Transition and Migration Approach Document'
54.0	17 December 2021	Modification to the SEC as directed by the Secretary of State pursuant to Section X5 and Condition 22 of the DCC Licence.	Amendments to: • SEC Section A 'Definitions and Interpretation' • SEC Appendix AM 'SMETS1 Supporting Requirements' Implementation of: • SEC Appendix AT 'SMETS1 Cryptographic Key Management Policy'
55.0	23 December 2021	Implementation of a Modification Proposal approved by the Change Board.	Amendments to SEC Section F 'Smart Metering System Requirements' This is due to the implementation of Modification Proposal MP188'
56.0	27 January 2022	Implementation of a Modification Proposal approved by the Change Board.	Amendments to SEC Schedule 11 'TS Applicability Tables' due to the implementation of Modification Proposal MP191.
57.0	24 February 2022	February 2022 SEC Release Implementation of Modification Proposals approved by the Change Board.	Amendments to: • Section A • Section G • Section H • Section K • Schedule 7 • Schedule 11 • Appendix A • Appendix B • Appendix C • Appendix D

			• Appendix J • Appendix K • Appendix L • Appendix M • Appendix N • Appendix O • Appendix P • Appendix Q • Appendix S • Appendix T • Appendix U • Appendix V • Appendix W • Appendix X • Appendix AC due to the implementation of Modification Proposals MP116, MP121, MP173, MP179 and MP196.
58.0	15 March 2022	Modification to the SEC as directed by the Secretary of State pursuant to Section X5 and Condition 22 of the DCC Licence.	Amendments to SEC Appendix AL 'SMETS1 Transition and Migration Approach Document'
59.0	24 March 2022	Implementation of a Modification Proposal approved by the Change Board.	Amendments to: • SEC Section A 'Definitions and Interpretation' • SEC Schedule 11 'TS Applicability Tables
60.0	10 June 2022	Modification to the SEC as directed by the Secretary of State pursuant to Section X5 and Condition 22 of the DCC Licence.	Amendments to: • SEC Appendix J 'Enduring Testing Approach Document' • SEC Appendix AK 'SEC Variation Testing Approach Document for SMETS1 Services' • SEC Appendix AL 'SMETS1 Transition and Migration Approach Document'
61.0	30 June 2022	June 2022 SEC Release Implementation of Modification Proposals approved by the Change Board and the Authority.	Amendments to: • SEC Section A 'Definitions and Interpretation' • SEC Section G 'Security' • SEC Section J 'Charges' • SEC Schedule 11 'TS

		Modification to the SEC as directed by the Secretary of State pursuant to Section X5 and Condition 22 of the DCC Licence.	Applicability Tables' • SEC Appendix AB 'Service Request Processing Document' Implementation of: • SEC Appendix AD 'DCC User Interface Specification' v5.1
62.0	18 July 2022	Implementation of a Modification Proposal approved by the Authority.	Amendments to: • SEC Section A 'Definitions and Interpretation' • SEC Section E 'Registration Data' • SEC Section G 'Security' • SEC Section H 'DCC Services' • SEC Section K 'Charging Methodology' • SEC Section L 'Smart Metering Key Infrastructure and DCC Key Infrastructure' • SEC Section P 'Production Proving' • SEC Appendix X 'Registration Data Interface Specification' • SEC Appendix Y 'Registration Data Interface Code of Connection' • SEC Appendix AG 'Incident Management Policy' • SEC Appendix AL 'SMETS1 Transition and Migration Approach Document'
63.0	1 August 2022	Implementation of a Modification Proposal approved by the Change Board.	Amendments to: • SEC Section F 'Smart Metering System Requirements' • SEC Appendix Z 'CPL Requirements Document' due to the implementation of Modification Proposal MP209. Corrections to SEC Section L

			'Smart Metering Key Infrastructure and DCC Key Infrastructure'.
64.0	12 October 2022	Implementation of a Modification Proposal approved by the Authority.	Amendments to: • SEC Section A 'Definitions and Interpretation' • SEC Section H 'DCC Services' due to the implementation of Modification Proposal MP096.
65.0	3 November 2022	November 2022 SEC Release Implementation of Modification Proposals approved by the Change Board and the Authority.	Amendments to: • SEC Section A • SEC Section C • SEC Section F • SEC Section G • SEC Section H • SEC Section J • SEC Section K • SEC Section L • SEC Section M • SEC Section P • SEC Section T • SEC Section X • SEC Section Z • SEC Schedule 5 • SEC Schedule 6 • SEC Schedule 7 • SEC Schedule 8 • SEC Schedule 9 • SEC Schedule 10 • SEC Schedule 11 • SEC Appendix B • SEC Appendix D • SEC Appendix E • SEC Appendix G • SEC Appendix H • SEC Appendix I • SEC Appendix J • SEC Appendix L • SEC Appendix O • SEC Appendix S • SEC Appendix X • SEC Appendix Z • SEC Appendix AA • SEC Appendix AB • SEC Appendix AG • SEC Appendix AI • SEC Appendix AJ • SEC Appendix AL • SEC Appendix AN

			• SEC Appendix AO • SEC Appendix AP 'FOC S1SPKI Certificate Policy' • SEC Appendix AP 'Secure S1SPKI Certificate Policy' • SEC Appendix AQ • SEC Appendix AS • SEC Appendix AT
66.0	20 December 2022	Modification to the SEC as directed by the Secretary of State pursuant to Section X5 and Condition 22 of the DCC Licence.	Amendments to: • SEC Appendix AL 'SMETS1 Transition and Migration Approach Document'
67.0	26 January 2023	Implementation of a Modification Proposal approved by the Change Board.	Amendments to: • SEC Schedule 11 'TS Applicability Tables' due to the implementation of Modification Proposal MP221.
68.0	21 February 2023	Modification to the SEC as directed by the Secretary of State pursuant to Section X5 and Condition 22 of the DCC Licence.	Amendments to: • SEC Appendix AL 'SMETS1 Transition and Migration Approach Document'
69.0	23 February 2023	February 2023 SEC Release Implementation of Modification Proposals approved by the Change Board.	Amendments to: • SEC Section A • SEC Section D • SEC Section E • SEC Section F • SEC Section H • SEC Section L • SEC Section T • SEC Section X • SEC Section Z • SEC Appendix K • SEC Appendix Z • SEC Appendix AC • SEC Appendix AJ
70.0	21 March 2023	Modification to the SEC as directed by the Secretary of State pursuant to Section X5 and Condition 22 of the DCC Licence.	Amendments to: • SEC Appendix AL 'SMETS1 Transition and Migration Approach Document'
71.0	22 March 2023	Implementation of a Modification Proposal	Amendments to: • SEC Appendix L 'SMKI

		approved by the Change Board.	Recovery Procedure' due to the implementation of Modification Proposal MP198. Corrections to SEC Section G 'Security'.
72.0	17 April 2023	Implementation of a Modification Proposal approved by the Change Board.	Amendments to: • SEC Schedule 11 'TS Applicability Tables' due to the implementation of Modification Proposal MP227.
73.0	17 May 2023	Modification to the SEC as directed by the Secretary of State pursuant to Section X5 and Condition 22 of the DCC Licence.	Amendments to: • SEC Appendix AL 'SMETS1 Transition and Migration Approach Document'
74.0	23 May 2023	Modification to the SEC as directed by the Secretary of State pursuant to Section X5 and Condition 22 of the DCC Licence.	Amendments to: • SEC Appendix AM 'SMETS1 Supporting Requirements'
75.0	08 June 2023	Modification to the SEC as directed by the Secretary of State pursuant to Section X5 and Condition 22 of the DCC Licence.	Amendments to: • SEC Section A • SEC Section D • SEC Section F • SEC Section G • SEC Section K • SEC Section L • SEC Section M • SEC Section X
76.0	29 June 2023	June 2023 SEC Release Implementation of Modification Proposals approved by the Change Board and the Authority. Modification to the SEC as directed by the Secretary of State pursuant to Section X5 and Condition 22 of the DCC Licence.	Amendments to: • SEC Section F • SEC Section G • SEC Section H • SEC Section L • SEC Schedule 11 • SEC Appendix B • SEC Appendix E • SEC Appendix Z • SEC Appendix AA • SEC Appendix AB • SEC Appendix AC • SEC Appendix AS Implementation of: • SEC Appendix AD 'DCC

			- User Interface Specification' v5.2 - SEC Appendix AF 'Message Mapping Catalogue' v5.2
77.0	11 September 2023	Implementation of a Modification Proposal approved by the Change Board.	Amendments to: - SEC Section A - SEC Section L - SEC Appendix D - SEC Appendix Q due to the implementation of Modification Proposal MP168.
78.0	15 September 2023	Modification to the SEC as directed by the Secretary of State pursuant to Section X5 and Condition 22 of the DCC Licence.	Amendments to: - SEC Appendix AL 'SMETS1 Transition and Migration Approach Document'
79.0	02 November 2023	November 2023 SEC Release Implementation of Modification Proposals approved by the Change Board.	Amendments to: - SEC Section A - SEC Section G - SEC Section H - SEC Section I - SEC Schedule 8 - SEC Schedule 9 - SEC Schedule 11 - SEC Appendix A - SEC Appendix B - SEC Appendix C - SEC Appendix D - SEC Appendix Q - SEC Appendix W - SEC Appendix AG - SEC Appendix AP2 due to the implementation of Modification Proposals MP122B, MP216, MP226, MP245, MP249 and MP250.
80.0	06 December 2023	Modification to the SEC as directed by the Secretary of State pursuant to Section X5 and Condition 22 of the DCC Licence.	Implementation of: - SEC Appendix AU 'Network Evolution Transition and Migration Approach Document'
81.0	18 December 2023	Modification to the SEC as directed by the Secretary of State pursuant to Section X5	Amendment to: - Appendix AL 'SMETS1 Transition and Migration Approach Document'

		and Condition 22 of the DCC Licence.	
82.0	20 December 2023	Implementation of a Modification Proposal approved by the Change Board.	Amendments to: • SEC Appendix S 'DCCKI Certificate Policy' due to the implementation of Modification Proposal MP251
83.0	09 January 2024	Modification to the SEC as directed by the Secretary of State pursuant to Section X5 and Condition 22 of the DCC Licence.	Amendment to: • SEC Appendix AQ 'SEC Variation Testing Approach Document for the CH&N Arrangements v3.0'
84.0	27 February 2024	Modification to the SEC as directed by the Secretary of State pursuant to Section X5 and Condition 22 of the DCC Licence.	Amendment to: • SEC Appendix AK 'SEC Variation Testing Approach Document for SMETS1 Services'
85.0	29 February 2024	February 2024 SEC Release Implementation of Modification Proposals approved by the Change Board.	Amendments to: • SEC Section A • SEC Section D • SEC Section G • SEC Section H • SEC Section L • SEC Schedule 11 • SEC Appendix B • SEC Appendix M • SEC Appendix O • SEC Appendix R • SEC Appendix S • SEC Appendix T • SEC Appendix X • SEC Appendix AI • SEC Appendix AL due to the implementation of Modification Proposals MP162, MP167B, MP176, MP243, MP259 and MP261.
86.0	08 April 2024	Implementation of a Modification Proposal approved by the Change Board.	Amendments to: • SEC Section A • SEC Section F • SEC Appendix Z due to the implementation of Modification Proposal MP231.
87.0	15 April 2024	Implementation of a Modification Proposal	Amendment to: • SEC Section F

		approved by the Change Board.	due to the implementation of Modification Proposal MP264.

Dated: 23 September 2013

Smart Energy Code

Contents

Introduction

(A) This Code has been designated by the Secretary of State pursuant to the DCC Licence, and is subject to modification in accordance with the Secretary of State's statutory powers and the DCC Licence.

(B) The Parties comprise the DCC, Users (or prospective Users) of DCC's Services, and persons holding certain Energy Licences that are obliged by those licences to accede to this Code (some of whom are Users of DCC's Services).

(C) The Original Parties have agreed to give effect to, and to be bound by, this Code in accordance with the Framework Agreement.

(D) The other Parties have agreed to give effect to, and to be bound by, this Code in accordance with an Accession Agreement.

(E) SECCo is a company established to facilitate the operation of this Code. SECCo is not a Party (as defined), and only has rights and obligations under this Code where specified.

Version Control

The version control table showing the full history of changes to the Smart Energy Code and the reasons for those changes has been removed from the consolidated Code document due to its length. It is available to download here.

CONTENTS

SMART ENERGY CODE CONTENTS

Section E: Registration Data

Section F: Smart Metering System Requirements

Section G: Security

Section H: DCC Services

Section L: Smart Metering Key Infrastructure and DCC Key Infrastructure

Section M: General

Section N: SMETS1 Meters

Section P: Production Proving

Section T: Testing During Transition

Section X: Transition

Section Z: Alt HAN Arrangements

Schedules:

Appendices:

Appendix G: DCC Gateway Connection Code of Connection

Appendix H: CH Handover Support Materials

Appendix I: CH Installation and Maintenance Support Materials

Appendix J: Enduring Testing Approach Document

Appendix K: SMKI and Repository Test Scenarios Document

Appendix L: SMKI Recovery Procedure

Appendix M: SMKI Interface Design Specification

Appendix N: SMKI Code of Connection

Appendix O: SMKI Repository Interface Design Specification

Appendix P: SMKI Repository Code of Connection

Appendix Q: IKI Certificate Policy

Appendix R: Common Test Scenarios Document

Appendix S: DCCKI Certificate Policy

Appendix T: DCCKI Interface Design Specification

Appendix U: DCCKI Repository Interface Design Specification

Appendix V: DCCKI CoCo and DCCKI Repository CoCo

Appendix W: DCCKI Registration Authority Policies and Procedures

Appendix X: Registration Data Interface Specification

Appendix Y: Registration Data Interface Code of Connection

Appendix Z: CPL Requirements Document

Appendix AA: Threshold Anomaly Detection Procedures

Appendix AB: Service Request Processing Document

Appendix AC: Inventory, Enrolment and Decommissioning Procedures

Appendix AD: DCC User Interface Specification Version 1.1

Appendix AD: DCC User Interface Specification Version 2.0

Appendix AD: DCC User Interface Specification Version 3.0

Appendix AD: DCC User Interface Specification Version 3.1

Appendix AD: DCC User Interface Specification Version 4.0

Appendix AD: DCC User Interface Specification Version 5.0

Appendix AE: DCC User Interface Code of Connection

Appendix AF: Message Mapping Catalogue Version 1.0

Appendix AF: Message Mapping Catalogue Version 2.0

Appendix AF: Message Mapping Catalogue Version 3.0

Appendix AF: Message Mapping Catalogue Version 3.1

Appendix AF: Message Mapping Catalogue Version 4.0

Appendix AF: Message Mapping Catalogue Version 5.0

Appendix AG: Incident Management Policy

Appendix AH: Self Service Interface Access Control Specification

Appendix AI: Self Service Interface Code of Connection

Appendix AJ: SEC Variation Testing Approach Document

Appendix AK: SEC Variation Testing Approach Document for SMETS1 Services

Appendix AL: SMETS1 Transition and Migration Approach Document

Appendix AM: SMETS1 Supporting Requirements

Appendix AN: SEC Variation Testing Approach Document for BEIS Changes included in the November 2020 SEC Release

Appendix AO: S1SPKM Compliance Policy

Appendix AP1: Secure S1SPKI Certificate Policy

Appendix AP2: FOC S1SPKI Certificate Policy

Appendix AQ: SEC Variation Testing Approach Document for the CH&N Arrangements

Appendix AR: SEC Variation Testing Approach Document for the Enduring Change of Supplier Arrangements

Appendix AS: ECoS Transition and Migration Approach Document

Appendix AT: SMETS1 Cryptographic Key Management Policy

Appendix AU: Network Evolution Transition and Migration Approach Document

A DEFINITIONS AND INTERPRETATION

A1. DEFINITIONS

A1.1 In this Code, except where the context otherwise requires, the expressions in the left hand column below shall have the meanings given to them in the right hand column below:

4G Communications Hub means a Communications Hub which is capable of using 4G mobile cellular radio technology to connect to the SM WAN.

4G DBT Finance Acceleration Event means, in respect of each 4G DBT Finance Facility, that:

(a) an acceleration of repayment of the indebtedness thereunder occurs such that it is immediately due and payable by the borrower in circumstances where the DCC is liable for the same under the Direct Agreement; or

(b) the DCC becomes liable under the Direct Agreement to immediately pay the unamortised asset value (and any associated finance costs in respect) of any assets to which that facility relates.

4G DBT Finance Charges means, in respect of each 4G DBT Finance Facility, the DCC's charge to recover the applicable 4G DBT Finance Costs (being a subset of the Fixed Charges), in an amount each month determined by the DCC at the time it produces an Invoice for that month (having regard to the requirements of Condition 36.5 of the DCC Licence).

4G DBT Finance Costs means, in respect of each 4G DBT Finance Facility, the costs the DCC incurs in respect of that facility.

4G DBT Finance Facility means a facility, other than a Communications Hub Finance Facility, arranged by the DCC or a DCC Service Provider with an Approved Finance Party for the funding of the development costs (including design, build and testing costs) of any solutions or services which DCC procures in order to enable or facilitate its provision and/or operation of 4G Communications Hubs, such costs being incurred in respect of activities undertaken up to the point of volume manufacture of the 4G Communications Hubs (such point as further described in the plan produced pursuant to condition 13B of the DCC Licence), and being costs which DCC is entitled to recover via the Fixed Charges under this Code, including by way of a loan facility, an equity subscription, or an assignment or sale of receivables.

Acceptance Testing means testing of a software release undertaken by Users in order to determine whether the required specification for that software is met.

Access Control Broker means the DCC, acting in the capacity and exercising the functions of the Known Remote Party role identified as such in the GB Companion Specification.

Accession Agreement means an accession agreement entered into pursuant to Section B1 (Accession).

Acknowledgement means, in respect of a communication sent by a User to the DCC over the DCC User Interface, a communication by the DCC to the User via the DCC User Interface acknowledging receipt of the User's communication.

Additional Electricity Smart Meter means an Electricity Smart Meter which is installed at premises in such a manner and/or configuration that it:
(a) is joined to a Communications Hub Function at the premises; but
(b) is incapable of being used for the purposes of determining the quantity of electricity supplied to the premises.

Additional Registration Data means Electricity Additional Registration Data and Gas Additional Registration Data.

Additional Release Services has the meaning given to that expression in Section X1.17 (Testing in respect of Additional Release Services).

Additional SR Tests has the meaning given to that expression in Section X1.17 (Testing in respect of Additional Release Services).

Advanced Meter in relation to:
(a) an Electricity Meter, has the meaning given to that expression in standard condition 39 of the Electricity Supply Licence; and
(b) a Gas Meter, has the meaning given to that expression in standard condition 33 of the Gas Supply Licence.

Affected Party has the meaning given to that expression in the definition of Force Majeure.

Affiliate means, in relation to any person, any holding company of that person, any subsidiary of that person or any subsidiary of a holding company of that person, in each case within the meaning of section 1159 of the Companies Act 2006.

Alert
has the meaning given to ‘Alert’ in the GB Companion Specification.

Alert Management Mechanism
means the mechanism applied to Alerts received by the DCC, as described in clauses 17.8-17.10 of the Service Request Processing Document.

ALCS/HCALCS/APC/SAPC Labels List
has the meaning given to that expression in Section F11.1 (ALCS/HCALCS/APC/SAPC Labels List).

Alt HAN Arrangements
has the meaning given to that expression in condition 22.20(e) (Principal contents within the Smart Energy Code) of the DCC Licence.

Alt HAN Charges
means the Fixed Alt HAN Charges calculated in accordance with Section K5A or K6B (as applicable) taken together with the Explicit Charges in respect of the Explicit Charging Metrics at Section K7.5(t) and (u).

Alt HAN Forum
means the body of that name established in accordance with Section Z.1.1 (Establishment of the Alt HAN Forum).

Alt HAN Services
has the meaning given to that expression in Section Z6.1 (Definitions).

Alternate
has the meaning given to that expression in Section C5.19 (Alternates).

Alternative Installation End Date
has the meaning given to that expression in Section A4.2(c) (Derogations).

Alternative Solution
has the meaning given to that expression in Section D6.16 (Alternative Solutions).

Anomalous Event
means, in relation to any System, an activity or event that is not expected to occur in the course of the ordinary operation of that System.

Anomaly Detection Threshold means:

(a) in respect of a User ID used by a User in one or more of its User Roles, a number of communications within a period of time, where both that number and the period of time are set by the User in relation to that User ID;

(b) in respect of the DCC (including when acting as a SMETS1 Service Provider), either:
(i) a number of communications within a period of time, where both that number and the period of time are set by the DCC; or
(ii) a maximum or minimum data value within a communication, where that value is set by the DCC,in each case in accordance with the requirements of Section G6 applying (respectively) to the User or the DCC.

Applicability Period has the meaning given to that expression in Section A3.29(d) (GB Companion Specification and CPA Security Characteristics).

Applicant has the meaning given to that expression in Section B1.1 (Eligibility for Admission).

Application Association has the meaning given to that expression in the Green Book (DLMS UA 1000-2 Ed. 8), published by the DLMS User Association.

Application Fee has the meaning given to that expression in Section B1.5 (Application Fee).

Application Form means a form requesting the information set out in Schedule 5 (and which must not request any further information), in such format as the Code Administrator may determine from time to time.

Application Guidance has the meaning given to that expression in Section B1.4 (Application Form and Guidance).

Application Server means a software framework that enables software applications to be installed on an underlying operating system, where that software framework and operating system are both generally available either free of charge or on reasonable commercial terms.

Appropriate Permission means, in respect of a Communication Service or Local Command Service to be provided to a User in respect of a Smart Metering System at a premises that will result in the User obtaining Consumption Data, either:
(a) (where that User is the Import Supplier, Export Supplier, Gas Supplier,

Electricity Distributor or Gas Transporter for that Smart Metering System) that the User does not need consent to access that Consumption Data in accordance with its Energy Licence, or that the User has consent (whether explicit or implicit) in accordance with the requirements of its Energy Licence; or
(b) (where that User is not the Import Supplier, Export Supplier, Gas Supplier, Electricity Distributor or Gas Transporter for that Smart Metering System) that the Energy Consumer has given the User Unambiguous Consent to obtain that Consumption Data and such consent has not been withdrawn.

Appropriate Standard

has the meaning given to that expression in Section G3.28(b) (SMETS1 Smart Metering Systems).

Approved Budget

has the meaning given to that expression in Section C8.13 (Approval of Budgets).

Approved Finance Party

means, in respect of each DCC Finance Facility, the person with whom the DCC arranges the facility, or to whom the DCC accepts payment obligations under the Direct Agreement relating to that facility, as the case may be, and which has (from time to time) been notified by the DCC to the Authority and the Panel as meeting the requirements of this definition.

Associated

means:
(a) in respect of a Smart Meter, that the Smart Meter is identified in the Smart Metering Inventory as being associated with a Communications Hub Function; and
(b) in respect of any Device other than a Smart Meter or a Communications Hub Function, that the Device is identified in the Smart Metering Inventory as being associated with a Smart Meter or with a Gas Proxy Function,
and the expression "**Associate**" shall be interpreted accordingly.

Assurance Certificate

has the meaning given to that expression in Section F2.4 (Background to Assurance Certificates).

Assurance Certification Body

has the meaning given to that expression in Section F2.3 (Background to Assurance Certificates).

Authentication Key

has the meaning given to that expression in the Green Book (DLMS UA 1000-2 Ed. 8), published by the DLMS User Association.

Authorised Business in relation to the DCC, has the meaning given in the DCC Licence.

Authorised Subscriber means SECCo, a Party, a Manufacturer or an RDP which is an Authorised Subscriber for the purposes of (and in accordance with the meaning given to that expression in) any of the Certificate Policies.

Authority means the Gas and Electricity Markets Authority as established under section 1 of the Utilities Act 2000.

Authority Determined Modification has the meaning given to that expression in Section D2.6 (Authority Determined Modifications).

Authority-initiated Modification has the meaning given to that expression in Section D2.4 (Authority-initiated Modifications).

Authority-Led Modification Report has the meaning given to that expression in Section D9A.5 (Authority-Led Modification Report).

Authority-Led Variations means variations to this Code proposed by the Authority pursuant to a direction under Section D9A (Authority-Led Variations).

Back-Up means, in relation to Data which is held on any System, the storage of a copy of that Data for the purpose of ensuring that the copy may be used (if required) to restore or replace the original Data; and "Backed-Up" is to be interpreted accordingly.

Bank Guarantee means an on demand bank guarantee in a form reasonably acceptable to the DCC from a bank with the Required Bank Rating which guarantee has not been breached or disclaimed by the provider and has at least one month left until it expires.

Batched Certificate Signing Request has the meaning given to that expression in Section L8.2 (SMKI Services: Target Response Times).

BCDR Procedure means the Business Continuity and Disaster Recovery Procedure.

Bilateral Agreement means an agreement entered into pursuant to Section H7 (Elective Communication Services) between the DCC and a User.

BSC means the Balancing and Settlement Code maintained under the Electricity System Operator Licence.

Business Architecture means the business architecture which is designed to enable Parties to use the Services and/or to enable Parties, Energy Consumers and those acting on behalf of Energy Consumers to access the functionality described in the Technical Specifications.

Business Architecture Document means a document that describes the Business Architecture.

Business Continuity and Disaster Recovery Procedure means that part of the Incident Management Policy which describes the business continuity and disaster recovery procedures applicable to the Services.

Business Continuity and Disaster Recovery Test means a test of the operation of the DCC's disaster recovery and business continuity arrangements applicable to the Services.

Business Continuity and Disaster Recovery Test Schedule means a document created by the DCC setting out its schedule for undertaking a Business Continuity and Disaster Recovery Test and the likely duration of any such test.

Business Process means a combination of Service Requests as described in Section H13.1A or H13.1B (Code Performance Measures).

Cash Deposit means a deposit of funds by or on behalf of the User into a bank account in the name of the DCC, such that title in such funds transfers absolutely to the DCC.

Central Products List has the meaning given to that expression in Section F2.1 (Central Products List).

Centralised Registration Service has the meaning given to that term in the Smart Meter Communication Licence.

Certificate means a Device Certificate, DCA Certificate, Organisation Certificate, OCA Certificate, IKI Certificate or ICA Certificate (or, for the purposes of any Certificate Policy in which the term is defined, it shall have the meaning ascribed to it in that Certificate Policy).

Certificate Policy means the Device Certificate Policy, the Organisation Certificate Policy, or the IKI Certificate Policy.

Certificate Signing Request means a request for a Certificate submitted by an Eligible Subscriber in accordance with the SMKI RAPP.

Certified Cyber Professional (CPP) means the scheme of that name which is administered by NCSC, or any successor to that scheme.

Certified Cyber Security Consultancy (CCSC) means the scheme of that name which is administered by NCSC or any successor to that scheme.

Certified Products List means those entries on the Central Products List which identify SMETS2+ Device Models.

CESG means NCSC (and any reference to CESG in the Code shall be read as a reference to NCSC).

CH Batch Fault has the meaning given to that expression in Section F9.20 (Liquidated Damages for CH Batch Faults).

CH Batch Fault Payment has the meaning given to that expression in Section F9.21 (Liquidated Damages for CH Batch Faults).

CH Defect means, in respect of a Communications Hub, any fault or defect in relation to the Communications Hub (including any failure: to conform in all respects with, and be fit for the purposes described in, the CHTS; to be free from any defect in design, manufacture, materials or workmanship; and to comply with all applicable Laws and/or Directives including with respect to product safety), which is not caused by a breach of this Code by a Party other than the DCC.

CH Fault Diagnosis has the meaning given to that expression in Section F9.7 (CH Fault Diagnosis).

CH Handover Support Materials means, in respect of each Region, the SEC Subsidiary Document of that name set out in Appendix H and applying to that Region.

CH Installation and Maintenance Support Materials means, in respect of each Region, the SEC Subsidiary Document of that name set out in Appendix I and applying to that Region.

CH Order Management System means that part of the CH Ordering System described as the 'Order Management System' in the CH Handover Support Materials.

CH Ordering System has the meaning given to that expression in Section F5.20 (CH Ordering System).

CH Post-Installation DCC Responsibility has the meaning given to that expression in Section F9.6 (Categories of Responsibility).

CH Pre-Installation DCC Responsibility has the meaning given to that expression in Section F9.6 (Categories of Responsibility).

CH Support Materials means the CH Handover Support Materials and the CH Installation and Maintenance Support Materials.

CH Type Fault has the meaning given to that expression in Section F9.16 (Liquidated Damages for CH Type Faults).

CH Type Fault Payment has the meaning given to that expression in Section F9.19 (Liquidated Damages for CH Type Faults).

CH User Responsibility has the meaning given to that expression in Section F9.6 (Categories of Responsibility).

Change Board has the meaning given to that expression in Section D8.1 (Establishment of the Change Board).

Change Board Member has the meaning given to that expression in Section D8.4 (Membership of the Change Board).

Change Sub-Committee means the Sub-Committee established, or to whom the Panel has allocated the function of being such a Sub-Committee, pursuant to Section D2A (The Change Sub-Committee).

Charges means the charges payable to the DCC pursuant to this Code (including pursuant to Bilateral Agreements).

Charging Methodology means the methodology for determining the Charges, as set out in Section K (Charging Methodology).

Charging Objectives has the meaning given to that expression in Section C1 (SEC Objectives).

Charging Statement means, from time to time, the statement prepared by DCC pursuant to Condition 19 of the DCC Licence that is in force at that time.

CHECK means the scheme of that name which is administered by NCSC, or any successor to that scheme.

Check Cryptographic Protection means, in respect of any electronic Data, to check the Digital Signature(s) or Message Authentication Code within those Data (as applicable) using:

(a) the Public Key contained in the certificate issued by the relevant Certificate Authority associated with the Private Key of the person or device that those Data identify, or imply has generated the Digital Signature;

(b) where applicable, the recipient's relevant Private Key; and

(c) the relevant algorithm identified in the certificate policy under which the relevant certificates were issued (or, where such certificate or certificate policy does not exist, the appropriate algorithm).

CHTS means the Communications Hub Technical Specifications.

Citizens Advice means the National Association of Citizens Advice Bureaux.

Citizens Advice Scotland means the Scottish Association of Citizens Advice Bureaux.

Code means this Smart Energy Code (including its Schedules and the SEC Subsidiary Documents).

Code Administration Code of Practice means the document of that name as approved by the Authority from time to time.

Code Administration Code of Practice Principles means the principles set out as such in the Code Administration Code of Practice.

Code Administrator has the meaning given to that expression in Section C7.1 (Code Administrator).

Code Implementation SIT means the testing undertaken on implementation of this Code that tested the capability of the DCC and the component parts of the DCC Systems together with the Communications Hubs to interoperate with each other and with the RDP Systems.

Code Performance Measure means a performance measure set out in Section D11.3 (Code Performance Measures), Section H13.1 (Code Performance Measures) or Section L8.6 (Code Performance Measures).

Command means a communication to a Device in the format required by the GB Companion Specification and which incorporates all Digital Signatures and/or Message Authentication Codes required by the GB Companion Specification (or, in respect of a SMETS1Device, means an Instruction).

Commercial Activities includes, in particular, Energy Efficiency Services, Energy Management Services, Energy Metering Services, and Energy Price Comparison Services, in each case as defined in the DCC Licence and in relation to the Supply of Energy (or its use) under the Electricity Act and the Gas Act.

Commissioned means, in respect of a Device, that:

(a) the Device has been commissioned in accordance with the Smart

Metering Inventory Enrolment and Decommissioning Procedures or the Transition and Migration Approach Document; and
(b) the Device has not subsequently been Decommissioned or Suspended, and "**Commission**" is to be interpreted in accordance with (a) above. A Communications Hub shall be considered to be Commissioned where the Communications Hub Function that forms part of that Communications Hub is Commissioned.

Common Test Scenarios Document

means the SEC Subsidiary Document set out in Appendix R.

Communication Services

means the Core Communication Services or the Elective Communication Services.

Communications Hub

means a physical device that includes a Communications Hub Function together with a Gas Proxy Function.

Communications Hub Auxiliary Equipment

means any additional, replacement or spare equipment or packaging (not forming part of a Communications Hub) that may be required by a Supplier Party in relation to the installation, maintenance or return of a Communications Hub, as listed by the DCC on the CH Ordering System from time to time.

Communications Hub Charges

has the meaning given to the expression ‘Fixed CH Charges’ in Section K (Charging Methodology).

Communications Hub Finance Acceleration Event

means, in respect of each Communications Hub Finance Facility, that:
(a) an acceleration of repayment of the indebtedness thereunder occurs such that it is immediately due and payable by the borrower in circumstances where the DCC is liable for the same under the Direct Agreement; or
(b) the DCC becomes liable under the Direct Agreement to immediately pay the unamortised asset value (and any associated finance costs in respect) of the Communications Hubs to which that facility relates.

Communications Hub Finance Charges

means, in respect of each Communications Hub Finance Facility, the DCC’s charge to recover the applicable Communications Hub Finance Costs (being a subset of the Communications Hub Charges), in an amount each month determined by the DCC at the time it produces an Invoice for that month (having regard to the requirements of Condition 36.5 of the DCC Licence).

Communications Hub Finance Costs

means, in respect of each Communications Hub Finance Facility, the costs the DCC incurs in procuring the provision (but not the maintenance) of the tranche of Communications Hubs to which that facility relates.

Communications Hub Finance Facility

means a facility arranged by the DCC or a DCC Service Provider with an Approved Finance Party relating exclusively to the funding of the costs associated with acquiring and/or making available a tranche of Communications Hubs, including by way of a loan facility, an equity subscription, or an assignment or sale of receivables.

Communications Hub Forecast

has the meaning given to that expression in Section F5.2 (Communications Hub Forecasts).

Communications Hub Function

means either a SMETS1 CHF; or that part of a device installed (or to be installed) at a premises, which:
(a) consists of the components or other apparatus identified in; and
(b) as a minimum, has the functional capability specified by and complies with the other requirements of,
a Version of the CHTS (but excluding those provisions that are described as applying only to 'Gas Proxy Functions') which was within its Installation Validity Period on the date on which the device was installed.

Communications Hub Hot Shoe

means equipment, other than a Smart Meter, to which a Communications Hub can be connected (provided the Communications Hub complies with the ICHIS).

Communications Hub Order

has the meaning given to that expression in Section F5.7 (Communications Hub Orders).

Communications Hub Products

means, in respect of a Valid Communications Hub Order, the Communications Hubs of the applicable Device Models that are the subject of that order and/or the Communications Hub Auxiliary Equipment that is the subject of that order.

Communications Hub Services

means those Services described in Sections F5 (Communications Hub Forecasts & Orders), F6 (Delivery and Acceptance of Communications Hub), F7 (Installation and Maintenance of Communications Hubs), F8 (Removal and Return of Communications Hubs), and F9 (Categories of Communications Hub Responsibility).

Communications Hub Technical Specifications (or **CHTS**)

means the document(s) set out in Schedule 10.

Communications Hub Transfer

has the meaning given in Section F6A.1 (Communications Hub Transfers).

Communications Hub Transfer Request

has the meaning given in Section F6A.2 (Communications Hub Transfer Requests).

Competent Authority

means the Secretary of State, the Authority, and any local or regional or national agency, authority, department, inspectorate, minister, ministry, official or public or statutory person (whether autonomous or not) of the government of the United Kingdom (but only insofar as each has jurisdiction over the relevant Party, this Code or its subject matter).

Completion of Implementation

has the meaning given to that expression in Section X1 (General Provisions Regarding Transition).

Compromised

means:

(a) in relation to any System, that the intended purpose or effective operation of that System is compromised by the occurrence of any event which has an adverse effect on the confidentiality, integrity or availability of the System or of any Data that are stored on or communicated by means of it;

(b) in relation to any Device, that the intended purpose or effective operation of that Device is compromised by the occurrence of any event which has an adverse effect on the confidentiality, integrity or availability of the Device or of any Data that are stored on or communicated by means of it;

(c) in relation to any Data, that the confidentiality, integrity or availability of that Data is adversely affected by the occurrence of any event;

(d) in relation to any Secret Key Material, that that Secret Key Material (or any part of it), or any Cryptographic Module within which it is stored, is accessed by, or has become accessible to, a person not authorised to access it;

(e) in relation to any Certificate, that any of the following Private Keys is Compromised:

(i) the Private Key associated with the Public Key that is contained within that Certificate;

(ii) the Private Key used by the relevant Certification Authority to Digitally Sign the Certificate; or

(iii) where relevant, the Private Key used by the relevant Certification Authority to Digitally Sign the Certification Authority Certificate associated with the Private Key referred to in (ii);
(f) in relation to any DCCKI Certificate, that any of the following Private Keys is Compromised:
(i) the Private Key associated with the Public Key that is contained within that DCCKI Certificate;
(ii) the Private Key used by the DCCKICA to Digitally Sign
the DCCKI Certificate; or
(iii) where relevant, the Private Key used by the DCCKICA to Digitally Sign the DCCKICA Certificate associated with the Private Key referred to in (ii);
(g) in relation to any certificate issued under an S1SPKI (the 'end certificate'), that any of the following Private Keys is Compromised:
(i) the Private Key associated with the Public Key that is contained within that end certificate;
(ii) any other Private Key that has been used to Digitally Sign any certificate that may be used to link the end certificate to the root certificate for that S1SPKI; and
(h) in relation to any process or to the functionality of any hardware, firmware or software, that the intended purpose or effective operation of that process or functionality is compromised by the occurrence of any event which has an adverse effect on its confidentiality, integrity or availability,
(and “**Compromise**” and “**Compromising**” are to be interpreted accordingly).

Confidential Information

means, in respect of a Party other than DCC, the Data belonging or relating to that Party or that otherwise becomes available to the DCC as a result (whether directly or indirectly) of that Party being a party to this Code.

Confirm Validity

means:
(a) where the person carrying out the check has not previously done so in relation to a particular certificate, to successfully confirm the certificate path validation by using:
(i) the path validation algorithm specified in IETF RFC 5280; or
(ii) where the algorithm identified in IETF RFC 5280 is not appropriate for the certificate for which validity is being confirmed, such other certificate path validation as is appropriate in relation to that type of certificate; or
(b) where the person carrying out the check has previously carried out the check in paragraph (a) in relation to a particular certificate, that the certificate has not subsequently been revoked, and its validity period has not expired.

Consequential Change

means either (as the context requires) a Modification to this Code or a variation to another Energy Code, which (in either case) the Cross Code Steering Group considers would be necessary to give full and timely effect to a variation under a different Energy Code (if that variation was approved).

Consignment has the meaning given to that expression in Section F5.9 (Communications Hub Orders).

Consultation Summary has the meaning given to that expression in Section D6.14 (Working Group Consultation).

Consumer Data has the meaning given to that expression in Section M5.6 (Consumer Data).

Consumer Member has the meaning given to that expression in Section C3.1 (Panel Composition).

Consumer Prices Index means, in respect of any month, the consumer prices index (CPI) published for that month by the Office of National Statistics.

Consumption Data means, in respect of a premises, the quantity of electricity or gas measured by the Energy Meter as having been supplied to the premises.

Contingency Key Pair means Key Pair established by the DCC for the purposes of the replacement of Root OCA Certificates on Devices after a Relevant Private Key has been Compromised, and comprising:

a. a "**Contingency Private Key**", being the Private Key, which is part of that Key Pair; and

b. a "**Contingency Public Key**", being the Public Key which is part of that Key Pair and which is stored in the WrappedApexContingencyKey field of the Root OCA Certificate (being the field identified as such in the Root OCA Certificate Profile at Annex B of the Organisation Certificate Policy).

Contingency Private Key has the meaning given to that expression in sub-paragraph (a) of the definition of Contingency Key Pair in this Section A1.1.

Contingency Public Key has the meaning given to that expression in sub paragraph (b) of the definition of Contingency Key Pair in this Section A1.1.

Contingency Symmetric Key means the symmetric key used to decrypt the Contingency Public Key as set out in the GB Companion Specification.

Core Communication Services means the provision of the Services set out in the DCC User Interface Services Schedule, but excluding the Enrolment Services and Local Command Services.

Correlate means, in respect of one or more Pre-Commands received by a User from the DCC in respect of a Service Request sent by that User, carrying out a process to check that the relevant contents of the Pre-Command is substantively identical to that of the Service Request using either (at the User's discretion):
(a) the Parse and Correlate Software; or
(b) equivalent software procured or developed by the User in accordance with Good Industry Practice,
and "**Correlated**" shall be interpreted accordingly.

CoS Party means the DCC when performing the tasks ascribed to the CoS Party in the Service Request Processing Document.

Countersigned means, in respect of any electronic Data, that such Data have had a Digital Signature applied to them by the DCC in circumstances in which the DCC is required to 'Countersign' the Data, as described in the DCC User Interface Specification (and "**Countersign**" and "**Countersigning**" are to be interpreted accordingly).

Countersigned SMETS1 Alert has the meaning given to that expression in the DCC User Interface Specification.

Countersigned SMETS1 Response has the meaning given to that expression in the DCC User Interface Specification.

Countersigned S1SP Alert has the meaning given to that expression in the DCC User Interface Specification.

Countersigned Service Request means a communication sent by the DCC to a SMETS1 Service Provider in the circumstances set out in the Service Request Processing Document.

CPA Assurance Maintenance Plan means the document agreed with the NCSC that describes the components of a device which, if changed, will require a new CPA Certificate to be issued.

CPA Certificates has the meaning given to that expression in Section F2.4 (Background to Assurance Certificates).

CPA Certificate Remedial Plan means a remedial plan for resolving the security issues that have resulted in or arisen from (or will result in or arise from) the cancellation, withdrawal, or expiry without renewal, of a Device Model's CPA Certificate, as further described in the CPL Requirements Document.

CPA Security Characteristics means the documents published from time to time on the NCSC website that set out the features, testing and deployment requirements necessary to obtain a CPA Certificate in respect of one or more of the following:
(a) 'Gas Smart Metering Equipment';
(b) 'Electricity Smart Metering Equipment';
(c) 'Communications Hubs';
(d) 'HAN Connected Auxiliary Load Control Switches'.

CPL Requirements Document means the SEC Subsidiary Document of that name set out as Appendix Z.

Credit Assessment Agency means the Credit Assessment Agency named in the table at Section J3.14 (Party's Unsecured Credit Factor Percentage).

Credit Assessment Score means, in respect of a Party, a credit assessment score in respect of that Party procured from the Credit Assessment Agency.

Credit Cover Requirement has the meaning given to that expression in Section J3.4 (Amount of Credit Support to be Provided).

Credit Cover Minimum Threshold means, in respect of each Regulatory Year, £2,000, multiplied by the Consumer Prices Index for the October preceding the start of that Regulatory Year, divided by the Consumer Prices Index for October 2014. The relevant amount will be rounded to the nearest pound.

Credit Support means one or more of a Bank Guarantee, Cash Deposit and/or Letter of Credit procured by a User pursuant to Section J3 (Credit Cover Requirement).

CREST

means the not-for-profit company registered in the United Kingdom with company number 06024007.

Critical Command

has the meaning given to that expression in the GB Companion Specification.

Critical Service Request

means a Service Request which is identified as critical in the DCC User Interface Specification (or, in the case of Elective Communication Services, the relevant Bilateral Agreement).

Critical Service Response

means a Service Response in respect of a Critical Service Request.

Cross Code Steering Group

means the group of that name established under the Change Management Schedule of the REC.

Cryptographic Credential Token

means a token compliant with FIPS 140-2 Level 3 (or any equivalent to that Federal Information Processing Standard which updates or replaces it from time to time) and containing Secret Key Material, as issued in accordance with the SMKI RAPP.

Cryptographic Hash Function

means an algorithm:
(a) the inputs to which it would be computationally infeasible to determine from knowledge of its outputs; and
(b) in relation to which it would be computationally infeasible to find an input which generates the same output as any other input.

Cryptographic Module

means a set of hardware, software and/or firmware that is Separated from all other Systems and that is designed for:
(a) the secure storage of Secret Key Material; and
(b) the implementation of Cryptographic Processing without revealing Secret Key Material.

Cryptographic Processing

means the generation, storage (other than of Secret Key Material used in relation to communications with a SMETS1 Device, where that Secret Key Material is encrypted) or use of any Secret Key Material.

CSP System

means those parts of the DCC Total System which comprise Systems used by a DCC Service Provider in order to provide Communications Services.

CSS Provider

means the entity providing the Centralised Registration Service.

CSS Provider Systems

means any Systems which are operated by or on behalf of the CSS Provider, and which are used in whole or in part for:

(a) the collection, storage, Back-Up, processing or communication of Registration Data immediately prior to, or for the purposes of, its provision to the DCC Live System referred to paragraph (a) and paragraph (c) of the definition of DCC Live Systems; or

(b) generating Data for communication to the OCA, ICA or DCCKICA, or receiving Data from the OCA, ICA or DCCKICA (including any Systems which store or use Secret Key Material for such purposes),

and any other Systems from which the Systems described in paragraphs (a) and (b) are not Separated.

For the avoidance of doubt, CSS Provider Systems include only the Systems used by the CSS Provider to send Registration Data to the DCC and any other Systems from which those sending Systems are not Separate.

CSV file

has the meaning given to that expression in the Threshold Anomaly Detection Procedures.

Customer Analytics Reporting

means the reporting suite provided by the DCC to Users, the requirements of which are described in the Customer Analytics Reporting Methodology and Guidance Document.

Customer Analytics Reporting Methodology and Guidance Document

means the document of that name as established and from time to time updated by the DCC pursuant to Section H13.6A (Customer Analytics Reporting).

Customer Supply Continuity Plan

means the plan of that name maintained by each Supplier Party under Condition 19E of its Gas Supply Licence and/or Condition 19C of its Electricity Supply Licence.

Data

means any information, data, knowledge, figures, methodologies, minutes, reports, forecasts, images or sounds (together with any database made up of any of these) embodied in any medium (whether tangible or electronic).

Data Controller

has the meaning given to 'controller' in the Data Protection Legislation.

Data Processor has the meaning given to 'processor' in the Data Protection Legislation.

Data Protection Legislation means General Data Protection Regulation and any national legislation implementing the same and related statutory instruments.

Data Retention Policy means a document developed and maintained by a Party which sets out, in relation to Data held by that Party, the periods for which such Data will be held by it for the purpose of ensuring that it is able to satisfy its legal, contractual and commercial requirements in respect of the Data.

Data Subject has the meaning given to that expression in the Data Protection Legislation.

Data Subject Rights means the rights of Data Subjects under the Data Protection Legislation.

DCA Certificate has the meaning given to that expression in Annex A of the Device Certificate Policy.

DCC means, subject to Section M9 (Transfer of DCC Licence), the holder from time to time of the DCC Licence. In accordance with Section A2.1(l), references to the DCC shall (where applicable) include references to the DCC Service Providers with whom the DCC has contracted in order to secure performance of its obligations under this Code.

DCC Alert has the meaning given to that expression in the DCC User Interface Specification.

DCC Assessment means a DCC Preliminary Assessment or a DCC Impact Assessment.

DCC Boxed means a testing tool provided by the DCC that replicates parts of the DCC Total System which can be used by Testing Participants outside of the DCC's physical test laboratories.

DCC Finance Facility means a Communications Hub Finance Facility or a 4G DBT Finance Facility.

DCC Gateway Bandwidth Option means a DCC Gateway HV Connection or a DCC Gateway LV Connection.

DCC Gateway Connection means, for a premises, the physical infrastructure by which a connection is (or is to be) made between that premises and the DCC Systems (and each DCC Gateway Connection shall form part of the DCC Systems).

DCC Gateway Connection Code of Connection means the SEC Subsidiary Document set out in Appendix G.

DCC Gateway Equipment means, for each premises and any DCC Gateway Connection provided at that premises, that part of the DCC Gateway Connection that is (or is to be) located within that premises.

DCC Gateway HV Connection means the high-volume technology solution by which the DCC provides DCC Gateway Connections, as further described in the DCC Gateway Connection Code of Connection.

DCC Gateway LV Connection means the low-volume technology solution by which the DCC provides DCC Gateway Connections, as further described in the DCC Gateway Connection Code of Connection.

DCC Gateway Party means a Party that is seeking or has been provided with a DCC Gateway Connection at its premises, or to whom the right to use that connection has been transferred in accordance with Section H15.16 (Use of a DCC Gateway Connection)..

DCC ID means each identification number established by the DCC pursuant to Section H4.43 (DCC IDs).

DCC Impact Assessment means, in respect of analysis pursuant to Section D6.9 (Analysis by the DCC), a full and formal assessment by the DCC of the determined area for analysis.

DCC Independent Security Assessment Arrangements has the meaning given to that expression in Section G9.1 (The DCC Independent Security Assessment Arrangements).

DCC Independent Security Assessment Service Provider has the meaning given to that expression in Section G9.3 (Procurement of the DCC Independent Security Assessment Service Provider).

DCC Independent Security Assurance Service Provider

has the meaning given to that expression in Section G9.4 (The DCC Independent Security Assurance Service Provider).

DCC Individual Live System

means, with regard to the DCC's duty to Separate parts of the DCC Total System, a part of the DCC Total System which is used:
(a) for one of the purposes specified in paragraphs (a) to (g), or (j) of the definition of DCC Live Systems, where the part used for each such purpose shall be treated as an individual System distinct from:
(i) the part used for each other such purpose; and
(ii) any part used for a purpose specified in either paragraph (h) or (i) of the definition of DCC Live Systems; or
(b) by a SMETS1 Service Provider for the purpose specified in paragraph (h) of the definition of DCC Live Systems, where the part used by each SMETS1 Service Provider shall be treated as an individual System distinct from:
(i) the part used by each other SMETS1 Service Provider; and
(ii) any part used for a purpose specified in any of paragraphs (a) to (g), or paragraphs (i) and (j), of the definition of DCC Live Systems; or
(c) by a DCO for the purpose specified in paragraph (i) of the definition of DCC Live Systems, where the part used by each DCO shall be treated as an individual System distinct from:
(i) the part used by each other DCO; and
(ii) any part used for a purpose specified in any of paragraphs (a) to (h) or (j) of the definition of DCC Live Systems.

DCC Interfaces

means each and every one of the following interfaces:
(a) the DCC User Interface;
(b) the Registration Data Interface;
(c) the SMKI Repository Interface;
(d) the SMKI Services Interface;
(e) the Self-Service Interface; and
(f) the communications interfaces used for the purposes of accessing those Testing Services designed to be accessed via DCC Gateway Connections.

DCC Internal Security Controls

means security controls applied by the DCC in relation to SMETS1 Service Requests in a manner consistent with the End-To-End Security Architecture.

DCC Internal Systems

means those aspects of the DCC Total System for which the specification or design is not set out in this Code.

DCC IT Supporting Systems

means, with regard to the DCC’s duty to Separate parts of the DCC Total System, those parts of the DCC Total System which are used to support the DCC Live Systems and DCC IT Testing and Training Systems.

DCC IT Testing and Training Systems

means, with regard to the DCC's duty to Separate parts of the DCC Total System, those parts of the DCC Total System which are used to support the testing and training of DCC Personnel and third parties in relation to the provision of Services by the DCC.

DCC Key Infrastructure (or DCCKI)

means the public key infrastructure established by DCC to provide, amongst other things, transport layer security across DCC Gateway Connections.

DCC Licence

means the licences granted under section 6(1A) of the Electricity Act and section 7AB(2) of the Gas Act.

DCC Live Systems

means those parts of the DCC Total System which are used for the purposes of:

a. (other than to the extent to which the activities fall within paragraph (b), (c), (f), (g), (h), (i) or (j) below) processing (including Countersigning of SMETS1 Responses, SMETS1 Alerts and S1SP Alerts, but not Countersigning of SMETS1 Service Requests) Service Requests, Pre-Commands, Commands, Instructions, Service Responses and Alerts, holding or using Registration Data for the purposes of processing Service Requests and Signed Pre-Commands, and providing the Repository Service;
b. Threshold Anomaly Detection (other than that carried out by a DCO, a SMETS1 Service Provider or the CoS Party) and (other than to the extent to which the activity falls within paragraph (d), (f), (g), (h), (i) or (j) below) Cryptographic Processing relating to the generation and use of a Message Authentication Code and Countersigning SMETS1 Service Requests;
c. discharging the obligations placed on the DCC in its capacity as CoS Party;
d. providing SMKI Services;
e. the Self-Service Interface;
f. creating, using, storing or destroying the Contingency Private Key, the Contingency Symmetric Key or the Recovery Private Key (except where each such key is being stored in an unusable form because it is or is being split into multiple parts as described in Appendix L (SMKI Recovery Procedure) or in the Organisation CPS;
g. the Production Proving Systems;
h. discharging the obligations of any SMETS1 Service Provider in its capacity as such;
i. discharging the obligations of any DCO in its capacity as such; and
j. discharging the obligations of the CSS Provider in its capacity as such.

DCC Member

has the meaning given to that expression in Section C3.1 (Panel Composition).

DCC Personnel

means those persons who are engaged by the DCC, in so far as such persons carry out, or are authorised to carry out, any activity in relation to the Authorised Business.

DCC Preliminary Assessment

means, in respect of analysis pursuant to Section D6.9 (Analysis by the DCC):
(a) a preliminary assessment by the DCC of the determined area for analysis; and
(b) the costs and expenses that the DCC will incur in undertaking a DCC Impact Assessment in respect of the determined area for analysis.

DCC Release Management Policy

has the meaning given to that expression in Section H8.9 (Release Management).

DCC Security Assessment Report

has the meaning given to that expression in Section G9.7(a) (DCC Security Assessment Reports and Responses).

DCC Security Assessment Response

has the meaning given to that expression in Section G9.7(b) (DCC Security Assessment Reports and Responses).

DCC Service Provider

means an External Service Provider, as defined in the DCC Licence (but always excluding the DCC itself).

DCC Service Provider Contract

means, as between the DCC and each DCC Service Provider, any arrangement (however described) pursuant to which the DCC procures services for the purpose of providing the Services.

DCC Systems

means the DCC Total System, including the SMETS1 SM WAN and the SMETS2+ SM WAN, but excluding all Communications Hubs.

DCC Total System

means the Systems used by the DCC and/or the DCC Service Providers in relation to the Services and/or this Code, including the DCC User Interface, the SMETS1 SM WAN, the SMETS2+ SM WAN and Communications Hubs except for those Communications Hubs which are:
(a) SMETS1 CHs;

(b) neither installed nor in the possession of the DCC; and/or
(c) installed, but are not Commissioned.

DCC User Interface means the communications interface designed to allow the communications referred to in Section H3.3 (Communications to be sent via the DCC User Interface) to be sent between the DCC and Users.

DCC User Interface Code of Connection means the SEC Subsidiary Document of that name set out in Appendix AE.

DCC User Interface Services means the Services described in the DCC User Interface Services Schedule.

DCC User Interface Services Schedule means the SEC Subsidiary Document of that name set out in Appendix E.

DCC User Interface Specification means the SEC Subsidiary Document set out in Appendix AD.

DCC Website means the DCC's publicly available website (or, where the Panel and the DCC so agree, the Website).

DCCKI Authorised Subscriber means a Party or RDP which is a DCCKI Authorised Subscriber for the purposes of (and in accordance with the meaning given to that expression in) the DCCKI Certificate Policy.

DCCKI Authority Revocation List (or DCCKI ARL) has the meaning given to that expression in the DCCKI Certificate Policy.

DCCKI Certificate has the meaning given to that expression in the DCCKI Certificate Policy.

DCCKI Certificate Policy means the SEC Subsidiary Document of that name set out in Appendix S.

DCCKI Certificate Revocation List (or DCCKI CRL) has the meaning given to that expression in the DCCKI Certificate Policy.

DCCKI Certificate Signing Request

means a request for a DCCKI Certificate submitted by a DCCKI Eligible Subscriber in accordance with the DCCKI Certificate Policy and the DCCKI RAPP.

DCCKI Certification Authority (or DCCKICA)

has the meaning given to that expression in the DCCKI Certificate Policy.

DCCKI Certification Practice Statement (or DCCKI CPS)

has the meaning given to that expression in Section L13.37 (the DCCKI Certification Practice Statement).

DCCKI Code of Connection

means the SEC Subsidiary Document of that name set out in Appendix V, which:
(a) has the purpose described in Section L13.14 (DCCKI Code of Connection); and
(b) is originally to be developed pursuant to Sections L13.15 to L13.16 (DCCKI Interface Document Development).

DCCKI Document Set

has the meaning given to that expression in Section L13.33 (the DCCKI Document Set).

DCCKI Eligible Subscriber

has the meaning given to that expression in Section L13.8 (DCCKI Eligible Subscribers).

DCCKI Infrastructure Certificate

has the meaning given to that expression in the DCCKI Certificate Policy.

DCCKI Interface Design Specification

means the SEC Subsidiary Document of that name set out in Appendix T, which:
(a) has the purpose described in Section L13.13 (DCCKI Interface Design Specification); and
(b) is originally to be developed pursuant to Sections L13.15 to L13.16 (DCCKI Interface Document Development).

DCCKI Participants

means the DCC (acting in its capacity as the provider of the DCCKI Services), all DCCKI Subscribers and all DCCKI Relying Parties.

DCCKI PMA Functions

has the meaning given to that expression in Section L13.54 (the DCCKI PMA Functions).

DCCKI Registration Authority means the DCC, acting in its capacity as such for the purposes of (and in accordance with the meaning given to that expression in) the DCCKI Certificate Policy.

DCCKI Registration Authority Policies and Procedures (or DCCKI RAPP) means the SEC Subsidiary Document of that name set out in Appendix W, which is originally to be developed pursuant to Sections L13.35 to L13.36 (the DCCKI Registration Authority Policies and Procedures: Document Development).

DCCKI Relying Party means a person who, pursuant to the Code, receives and relies upon a DCCKI Certificate.

DCCKI Repository has the meaning given to that expression in Section L13.17 (the DCCKI Repository).

DCCKI Repository Code of Connection means the SEC Subsidiary Document of that name set out in Appendix V, which:

a. (a) has the purpose described in Section L13.28 (DCCKI Repository Code of Connection); and
b. (b) is originally to be developed pursuant to Sections L13.29 to L13.30 (DCCKI Repository Interface Document Development).

DCCKI Repository Interface has the meaning given to that expression in Section L13.26 (the DCCKI Repository Interface).

DCCKI Repository Interface Design Specification means the SEC Subsidiary Document of that name set out in Appendix U, which:
(a) has the purpose described in Section L13.27 (DCCKI Repository Interface Design Specification); and
(b) is originally to be developed pursuant to Sections L13.29 to L13.30 (DCCKI Repository Interface Document Development).

DCCKI Repository Service has the meaning given to that expression in Section L13.18 (the DCCKI Repository Service).

DCCKI SEC Documents has the meaning given to that expression in Section L13.34 (the DCCKI SEC Documents).

DCCKI Service Interface has the meaning given to that expression in Section L13.12 (the DCCKI Service Interface).

DCCKI Services has the meaning given to that expression in Section L13.1 (the DCCKI Services).

DCCKI Subscriber means, in relation to any DCCKI Certificate, a Party or RDP which has been Issued with and accepted that Certificate, acting in its capacity as the holder of the Certificate.

DCCKICA Certificate has the meaning given to that expression in the DCCKI Certificate Policy.

DCO means the DCC when carrying out the role and activities ascribed to a DCO in this Code; and where the DCC carries out that role and those activities by processing communications which relate to different SMETS1 Service Providers, it shall be treated as being a separate DCO in respect of the communications relating to each such SMETS1 Service Provider.

Decommissioned means, in respect of a Device that has previously been Commissioned, that the Device has been decommissioned in accordance with Section H6.1 (Decommissioning).

Default Interest Rate means, for any day, 8% above the base lending rate of the Bank of England at 13.00 hours on that day.

Defaulting Party has the meaning given to that expression in Section M8.1 (Events of Default).

Delivery Batch means all the Communications Hubs that were delivered pursuant to Section F6 (Delivery and 37 Acceptance of Communications Hubs) to a single location during a month (regardless of whether they were delivered pursuant to more than one Communications Hub Order by more than one Party).

Delivery Date has the meaning given to that expression in Section F5.8 (Communications Hub Orders).

Delivery Location has the meaning given to that expression in Section F5.8 (Communications Hub Orders).

Delivery Month has the meaning given to that expression in Section F5.8 (Communications Hub Orders).

Delivery Quantity has the meaning given to that expression in Section F5.8 (Communications Hub Orders).

Delivery Window means, for each delivery of Communications Hub Products to a Delivery Location, the time period on the applicable Delivery Date within which the DCC is to deliver the Communications Hub Products, as established in accordance with the CH Handover Support Materials.

Denial of Service Event means any unauthorised attempt to make any part of a System wholly or partially unavailable for use for a period of time.

Deployed Products List means the list published by the Panel pursuant to Section F2.10 (Deployed Products List).

Derogation has the meaning given to that expression at Section A4.2.

Designated Premises means Non-Domestic Premises defined as Designated Premises within the meaning given to that expression in the Electricity Supply Licences or the Gas Supply Licences.

Detailed Evaluation has the meaning given to that expression in Section H7.7 (Detailed Evaluation of Elective Communication Services).

Device means one of the following individual devices: (a) an Electricity Smart Meter; (b) a Gas Smart Meter; (c) a Communications Hub Function; (d) a Gas Proxy Function; (e) a Pre-Payment Meter Interface Device; (f) a HAN Connected Auxiliary Load Control Switch; (g) a Standalone Auxiliary Proportional Controller; and (h) any Type 2 Device.

Device Alert has the meaning given to that expression in the DCC User Interface Specification.

Device and User System Tests has the meaning given to that expression in Section H14.31 (Device and User System Tests).

Device Certificate has the meaning given to that expression in Annex A of the Device Certificate Policy.

Device Certificate Policy means the SEC Subsidiary Document of that name set out in Appendix A.

Device Certification Authority (or DCA) has the meaning given to that expression in Annex A of the Device Certificate Policy.

Device Certification Practice Statement (or Device CPS) has the meaning given to that expression in Section L9.8 (the Device Certification Practice Statement).

Device ID means:
(a) in relation to a SMETS2+ Device, the unique number by which an individual Device can be identified, as allocated to that Device in accordance with the applicable version of the GB Companion Specification; or
(b) in relation to a SMETS1 Device, the unique number complying with the SMETS1 Supporting Requirements and by which the Device can be identified.

Device Log means, in respect of a SMETS2+ Device (excluding Type 2 Devices), the electronic record within that Device which records the other Devices from which that Device can receive Data via the HAN. In respect of a SMETS1 Device, it shall have the meaning in the SMETS1 Supporting Requirements.

Device Model

a. subject to sub-paragraph (b), in respect of a Communications Hub or a Device (other than a Communications Hub Function or a Gas Proxy Function), the Manufacturer, the model, the hardware version and the firmware version of the Communications Hub or Device or,
b. in relation to a PPMID that is capable of forming part of either a SMETS1 Smart Metering System, or a SMETS2+ Smart Metering System, insofar as it relates to the PPMID forming part of a SMETS1 Smart Metering System; the Manufacturer of the PPMID, its model, its hardware version and its firmware version that is different to the

firmware version of the PPMID that forms part of a SMETS2+ Smart Metering System.

Device Security Credentials means:
(a) in respect of any SMETS2+ Device (other than a Type 2 Device), the Device's active Device Certificates and the electronic record within that Device of information from any other Certificates required to be held on the Device in order to execute the functionality of that Device specified in the GB Companion Specification;
(b) in respect of a SMETS1 Device, the Device Security Credentials required by the SMETS1 Supporting Requirements.

Device Type means, in respect of a Device, a generic description of the category of Devices into which the Device falls.

Device Zigbee Information Repository means a table established and maintained by the Panel that details Device Zigbee details and Device Zigbee information.

Digital Signature means, in respect of any electronic Data, a digital signature generated using:

(a) the entirety of those Data (excluding the digital signature itself and, to the extent specified in the code, any other parts of those Data);
(b) a Private Key; and
(c) the signature algorithm defined in the certificate profile in the certificate policy under which the certificate associated with that Private Key was issued or (where such certificate policy does not exist) the signature algorithm relevant to that certificate.

Digitally Signed means, in respect of any electronic Data, that such Data have had the necessary Digital Signatures applied to them (and "Digitally Sign" and "Digitally Signing" are to be interpreted accordingly).

Direct Agreement means, in respect of each Communications Hub Finance Facility or 4G DBT Finance Facility, any agreement entered into by the DCC in relation to that facility under which the DCC owes direct payment obligations.

Disaster means an event that causes one or more of the 'DCC Disaster Impacts' listed in the BCDR Procedure.

Dispute means any dispute or difference (of whatever nature) arising under, out of or in connection with this Code and/or any Bilateral Agreement.

DLMS Certificates has the meaning given to that expression in Section F2.4 (Background to Assurance Certificates).

DLMS User Association means the association of that name located in Switzerland (see - www.dlms.com).

Domestic Premises means premises at which a Supply of Energy is or will be taken wholly or mainly for domestic purposes, which is to be interpreted in accordance with Condition 6 of the relevant Energy Supply Licence.

Draft Budget has the meaning given to that expression in Section C8.11 (Preparation of Draft Budgets).

Draft Proposal has the meaning given to that expression in Section D1.2 (Modifications).

Dual Band Communications Hub has the meaning given to that expression in the CHTS.

Dual Band Communications Hub Configuration Tables means the technical document set out as an annex to Section F4 (Operational Functionality, Interoperability and Access for the DCC).

Due Date has the meaning given to that expression in Section J1.5 (Payment of Charges).

DUIS means the DCC User Interface Specification.

DUIS XML Schema means, in relation to any Version of the DCC User Interface Specification, the version of the DUIS XML Schema contained within it, as specified in the defined term 'DUIS XML Schema' in that Version of the DCC User Interface Specification.

EII DCCKICA Certificate has the meaning given to that expression in the DCCKI Certificate Policy.

EII DCCKICA Certificate Revocation List (or EII DCCKICA CRL)

has the meaning given to that expression in the DCCKI Certificate Policy.

ECoS Interface

means any one or more communications interface designed to allow communications to be sent between:

a. that part of the DCC Total System which is used for the purposes referred to in paragraph (c) of the definition of DCC Live Systems; and
b. any other System.

ECoS Interface Specification

means any one or more document which specifies the detailed format of communications which are to take place across an ECoS Interface.

ECoS Service Live Date

means the date on which the DCC achieves the milestone which is:

a. set out in the plan approved by the Secretary of State under and in accordance with Condition 13A of the DCC Licence; and
b. referred to (or identified as) 'ECoS Service Live' in that approved plan.

Elected Members

has the meaning given to that expression in Section C3.1 (Panel Composition).

Elective Communication Services

means the provision of communication services that are (or are to be) defined in a Bilateral Agreement (rather than the DCC User Interface Services Schedule) in a manner that involves communication via the SM WAN (provided that such services must relate solely to the Supply of Energy or its use).

Electricity Act

means the Electricity Act 1989.

Electricity Additional Registration Data

has the meaning given to that expression in Section E5.2 (Electricity Data).

Electricity Distribution Licence

means a licence granted, or treated as granted, under section 6(1)(c) of the Electricity Act.

Electricity Distributor means, for a Smart Metering System or a Device, the holder of the Electricity Distribution Licence for the network to which the relevant premises are connected.

Electricity Meter means any meter that conforms to the requirements of paragraph 2 of schedule 7 to the Electricity Act and is used for the purpose of measuring the quantity of electricity that is supplied to premises.

Electricity Network Party means a Party that holds an Electricity Distribution Licence.

Electricity Smart Meter means either a SMETS1 ESME; or a device (other than a SMETS1 ESME) installed (or to be installed) at a premises, which:
(a) consists of the components or other apparatus identified in; and
(b) as a minimum, has the functional capability specified by and complies with the other requirements of,
the ESMETS (and, where applicable, the part(s) of the ESMETS relevant to the Physical Device Type in question) in a Version of the ESMETS which was within its Installation Validity Period on the date on which the device was installed.

Electricity Smart Metering Equipment Technical Specification (or **ESMETS)** means the part(s) of the document(s) set out in Schedule 9 identified as applying either to 'Electricity Smart Metering Equipment' or to 'Electricity Smart Metering System'.

Electricity Supplier Party means a Party that holds an Electricity Supply Licence (regardless of whether that Party also holds a Gas Supply Licence).

Electricity Supply Licence means a licence granted, or treated as granted, pursuant to section 6(1)(d) of the Electricity Act.

Eligible Subscriber has the meaning given to that expression in Section L3.15 (Eligible Subscribers).

Eligible User means, in respect of a Service set out in the DCC User Interface Services Schedule or an Elective Communication Service and (in either case) a Smart Metering System (or a Device forming, or to form, part of a Smart Metering System), one of the Users eligible to receive that Service in respect of that Smart Metering System (or such a Device), as further described in Section H3.8 (Eligibility for Services).

Eligible User Role means, in respect of a Service set out in the DCC User Interface Services Schedule or an Elective Communication Service, one of the User Roles that is capable of being an Eligible User in respect of that Service (determined without reference to a particular Smart Metering System or Device).

Enabling Services means one or more of the Enrolment Service, the Communications Hub Service, and the Other Enabling Services.

Encrypt means, in respect of Section H4 (Processing Service Requests), the process of encoding Data using the methods set out for that purpose in the GB Companion Specification; and "**Encrypted**" shall be interpreted accordingly.

End-to-End Security Architecture means a document that describes how the security controls in respect of smart metering relate to the architecture of the End-to-End Smart Metering System.

End-to-End Smart Metering System means the DCC Total System, all Enrolled Smart Metering Systems, all User Systems and all RDP Systems.

End-to-End Technical Architecture means the DCC Systems and the Smart Metering Systems together, including as documented in the Technical Code Specifications.

Enduring Change of Supplier Transition and Migration Approach Document (ETMAD) means the SEC Subsidiary Document set out in Appendix AS.

Enduring Testing Approach Document means the SEC Subsidiary Document set out in Appendix J.

Energy Code means a multilateral code or agreement maintained pursuant to one or more of the Energy Licences.

Energy Consumer means a person who receives, or wishes to receive, a Supply of Energy at any premises in Great Britain.

Energy Licence means a licence that is granted, or treated as granted, under section 6 of the Electricity Act or under section 7, 7A or 7AB of the Gas Act.

Energy Market Data Item means the most granular level of data defining a specific attribute in respect of a data type, the permissible values for which are defined and controlled in the Energy Market Data Specification.

Energy Market Data Specification a common set of standards for all industry data represented within the Energy Market Architecture Repository as defined in the REC.

Energy Market Message has the meaning given to that expression in the REC.

Energy Market Meta Data Owner means the organisation responsible for the control of the meta data associated with the Energy Market Data Item or Energy Market Message as defined in the REC.

Energy Meter means an Electricity Meter or a Gas Meter.

Energy Supply Licence means an Electricity Supply Licence or a Gas Supply Licence.

Enrolment means, in respect of a Smart Metering System, the act of enrolling that Smart Metering System in accordance with the Enrolment Service (and the words “**Enrol**” and “**Enrolled**” will be interpreted accordingly).

Enrolment Service means the Service described in Section H5 (Enrolment Services and the Smart Metering Inventory).

Equivalent Steps means in relation to a SMETS1 Device and/or a SMETS1 Service Request, those steps that are required to be taken such that:
(a) the relevant Device is, or Data relating to it, are configured or reconfigured; or
(b) Data that are stored on, or in relation to or generated by, that Device are retrieved,
so as to have an effect that is equivalent to that which would occur were a Service Request of the same Service Reference Variant as the SMETS1 Service Request to be Successfully Executed on a SMETS2+ Device equivalent to the SMETS1 Device (taking into account the different design functionality of the SMETS1 Device and, where relevant, any specific requirements for alternative processing set out in the SMETS1 Supporting

Requirements), and such that the appropriate SMETS1 Response(s) and SMETS1 Alert(s) can be generated, and provided that, in relation to a SMETS1 Device that has a Non-EPCL Device Model, the steps required to be taken shall be those steps of the nature set out above that would be required to have been taken in relation to that Device prior to its firmware version changing to that of a Non-EPCL Device Model.

EU Regulations means any retained EU Law.

EUI-64 Compliant means a 64-bit globally unique identifier governed by the Institute of Electrical and Electronics Engineers.

Event of Default has the meaning given to that expression in Section M8.1 (Events of Default).

Export MPAN means an MPAN for a Metering Point relating to the export of electricity from a premises.

Export Supplier means, for a Smart Metering System or a Device and any period of or point in time, the Supplier Party Registered during that period of or at that point in time in respect of the Export MPAN relating to that Smart Metering System or Device (but excluding Smart Metering Systems or Devices for which there is no related Import MPAN, in which circumstance such Registered Supplier Party is deemed to be the Import Supplier in accordance with the definition thereof).

Failing Electricity Supplier Party means an Electricity Supply Party whose Electricity Supply Licence is to be revoked by the Authority, as notified by the Authority to the SMKI PMA.

Failing Energy Supplier means a Supplier Party which is a Failing Gas Supplier Party and/or a Failing Electricity Supplier Party.

Failing Gas Supplier Party means a Gas Supplier Party whose Gas Supply Licence is to be revoked by the Authority, as notified by the Authority to the SMKI PMA.

Fast-Track Modifications has the meaning given to that expression in Section D2.8 (Fast-Track Modifications).

File Signing Certificate has the meaning given to that expression in the IKI Certificate Policy.

File Signing Software means software provided by the DCC for the purposes of enabling a Party to apply a Digital Signature to a CSV File.

Firmware Hash means the result of the application of a hash function, such function being a repeatable process to create a fixed size and condensed representation of a message using the SHA-256 algorithm as specified in the US Government's Federal Information Processing Standards document 180-4.

Firmware Information Repository means a table established and maintained by the Panel that details firmware updates, releases, Manufacturer contact details and other firmware information.

Follow-up Security Assessment has the meaning given to that expression in Section G8.19 (Categories of Security Assurance Assessment) for a User Security Assessment and in Section G9.17 for a DCC Security Assessment.

Force Majeure means, in respect of any Party (the **Affected Party**), any event or circumstance which is beyond the reasonable control of the Affected Party, but only to the extent such event or circumstance (or its consequences) could not have been prevented or avoided had the Affected Party acted in accordance with Good Industry Practice. Neither lack of funds nor strikes or other industrial disturbances affecting only the employees of the Affected Party and/or its contractors shall be interpreted as an event or circumstance beyond the Affected Party's control.

Forum Sub-Group has the meaning given to that expression in Section Z6.1 (Definitions).

Framework Agreement means an agreement in the form set out in Schedule 1.

Full Privacy Assessment has the meaning given to that expression in Section I2.12 (Categories of Assessment).

Full User Security Assessment has the meaning given to that expression in Section G8.16 (Categories of Security Assurance Assessment).

Future-Dated Services has the meaning given to that expression in Section H3.11 (Categories of Services).

Gas Act means the Gas Act 1986.

Gas Additional Registration Data has the meaning given to that expression in Section E5.4 (Gas Data).

Gas Meter means a meter that conforms to the requirements of section 17(1) of the Gas Act for the purpose of registering the quantity of gas supplied through pipes to premises.

Gas Network Party means a Party that holds a Gas Transporter Licence.

Gas Proxy Function means either a SMETS1 GPF; or a Device installed (or to be installed) at a premises, which:
(a) consists of the components or other apparatus identified in; and
(b) as a minimum, has the functional capability specified by and complies with the other requirements of,
a Version of the CHTS (but only those provisions that are described as applying to 'Gas Proxy Functions') which was within its Installation Validity Period on the date on which the device was installed.

Gas Smart Meter means either a SMETS1 GSME; or a device (other than a SMETS1 GSME) installed (or to be installed) at a premises, which:
(a) consists of the components or other apparatus identified in; and
(b) as a minimum, has the functional capability specified by and complies with the other requirements of,
a Version of the GSMETS which was within its Installation Validity Period on the date on which the device was installed.

Gas Smart Metering Equipment Technical Specification (or **GSMETS**) means the part(s) of the document(s) set out in Schedule 9 identified as applying either to 'Gas Smart Metering Equipment' or to 'Gas Smart Metering System'.

Gas Supplier means, for a Smart Metering System or a Device and any period of or point in time, the Supplier Party Registered during that period of or at that point in time in respect of the MPRN relating to that Smart Metering System or Device.

Gas Supplier Party means a Party that holds a Gas Supply Licence (regardless of whether that Party also holds an Electricity Supply Licence).

Gas Supply Licence means a licence granted, or treated as granted, pursuant to section 7A(1) of the Gas Act.

Gas Transporter means, for a Smart Metering System or a Device, the holder of the Gas Transporter Licence for the network to which the relevant premises are connected.

Gas Transporter Licence means a licence granted, or treated as granted, under section 7 of the Gas Act (but not the licence in respect of the National Transmission System, as defined in the UNC).

GB Companion Specification (or GBCS) means the document of that name set out in Schedule 8.

GBCS Payload means the content of a Pre-Command, Signed Pre-Command, Service Response or Device Alert which is set out in the format required by the GB Companion Specification.

General Data Protection Regulation means EU Regulation 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data.

General Installation End Date has the meaning given to that expression in Section A3.13.

General SEC Objectives has the meaning given to that expression in Section C1 (SEC Objectives).

GFI Testing means a testing service provided by the DCC to enable eligible persons to test the interoperability of Devices (other than those comprising Communications Hubs) with the DCC Systems and with the Communications Hubs to be provided as part of the Testing Services, such that those Devices are able to respond to Commands received from or via the DCC in accordance with the requirements defined in the GB Companion Specification.

GFI Testing Tools means a product provided by the DCC to enable Testing Participants to test their products against an interpretation of DCC Total Systems, including an interpretation of the GBCS standard, such that those Devices are able to respond to Commands received in accordance with the requirements defined in the GB Companion Specification.

Good Industry Practice means, in respect of a Party, the exercise of that degree of skill, diligence, prudence and foresight which would reasonably and ordinarily be expected from a skilled and experienced person engaged in a similar type of undertaking as that Party under the same or similar circumstances.

Greenhouse Gas Emissions means emissions of Greenhouse Gases, as defined in section 92 of the Climate Change Act 2008.

HAN means, for each Smart Metering System, the home area network created by the Communications Hub Function forming part of that Smart Metering System.

HAN Connected Auxiliary Load Control Switch means a device installed (or to be installed) at a premises, which:
(a) consists of the components or other apparatus identified in; and
(b) as a minimum, has the functional capability specified by and complies with the other requirements of,
a Version of the HCALCS Technical Specification which was within its Installation Validity Period on the date on which the device was installed.

HAN Requirements means the requirements with respect to the HAN provided for in the Energy Licences and this Code.

HAN Variants means the variations of SMETS2+ Communications Hub that are necessary to enable communication via each HAN Interface (as defined in the CHTS).

Hash means the result of the application of a hash function, such function being a repeatable process to create a fixed size and condensed representation of a message using the SHA-256 algorithm as specified in the US Government's Federal Information Processing Standards document 180-4.

HCALCS means a HAN Connected Auxiliary Load Control Switch.

HCALCS Technical Specification (or **HCALCSTS)** means the part(s) of the document(s) set out in Schedule 9 identified as applying to 'HAN Connected Auxiliary Load Control Switches'.

ICA Certificate has the meaning given to that expression in the IKI Certificate Policy.

ICHIS means the Intimate Communications Hub Interface Specifications.

ID Allocation Procedure means the document of that name developed and maintained in accordance with Section B2.2 (ID Allocation Procedure).

IETF RFC 5280 has the meaning given to that expression in the GB Companion Specification.

IHD means a device provided (or to be provided) at a premises, which is either a SMETS1 IHD; or:
(a) consists of the components or other apparatus identified in; and
(b) as a minimum, has the functional capability specified by and complies with the other requirements of,
a Version of the IHD Technical Specification which was within its Installation Validity Period on the date on which the device was provided, and which a User acting in the role of Import Supplier or Gas Supplier has joined, or is seeking to join, to an Electricity Smart Meter or Gas Proxy Function (as applicable).

IHD Technical Specification (or **IHDTS)** means the part(s) of the document(s) set out in Schedule 9 identified as applying to 'IHDs'.

IKI Authority Revocation List (or IKI ARL) has the meaning given to that expression in the IKI Certificate Policy.

IKI Certificate has the meaning given to that expression in the IKI Certificate Policy.

IKI Certificate Policy means the SEC Subsidiary Document of that name set out in Appendix Q.

IKI Certificate Revocation List (or IKI CRL) has the meaning given to that expression in the IKI Certificate Policy.

IKI Certification Practice Statement (or IKI CPS) has the meaning given to that expression in Section L9.20 (the IKI Certification Practice Statement).

IKI File Signing Certificate means an IKI Certificate issued by the IKI File Signing Certification Authority.

IKI File Signing Certification Authority has the meaning given to that expression in the IKI Certificate Policy.

Import MPAN means an MPAN for a Metering Point relating to the import of electricity to a premises.

Import Supplier means, for a Smart Metering System or a Device and any period of or point in time:

(a) the Supplier Party Registered during that period of or at that point in time in respect of the Import MPAN relating to that Smart Metering System or Device; or

(b) where there is no related Import MPAN for that Smart Metering System or Device, the Supplier Party Registered during that period of or at that point in time in respect of the Export MPAN relating to that Smart Metering System or Device.

Incident means an actual or potential interruption to (or reduction in the quality or security of) the Services, as further described in the Incident Management Policy.

Incident Category has the meaning given to that expression in Section H9.1 (Incident Management Policy).

Incident Management means a framework of processes designed to identify, raise, allocate responsibility for, track and close Incidents.

Incident Management Log has the meaning given to that expression in Section H9.3 (Incident Management Log).

Incident Management Policy means the SEC Subsidiary Document of that name set out in Appendix AG.

Incident Parties has the meaning given to that expression in Section H9.1 (Incident Management Policy).

Independent Assurance Scheme has the meaning given to that expression in Part 2.1 of the SMKI Compliance Policy (DCC: Duty to Submit to an Independent Assurance Scheme).

Independent Privacy Auditor has the meaning given to that expression in Section I2.1 (Procurement of the Independent Privacy Auditor).

Independent SMKI Assurance Service Provider has the meaning given to that expression in Part 3.1 of the SMKI Compliance Policy (DCC: Duty to Procure Independent Assurance Services).

Independent S1SPKM Assurance Service Provider has the meaning given to that expression in the S1SPKM Compliance Policy (DCC: Duty to Procure Independent Assurance Services).

Independent Time Source has the meaning given to that expression in Section G2.46(b) (Network Time).

Information Classification Scheme means a methodology for:
(a) the appropriate classification of all Data that are processed or stored on a System by reference to the potential impact of those Data being Compromised; and
(b) determining the controls to be applied to the processing, storage, transfer and deletion of each such class of those Data.

Information Commissioner means the Commissioner as defined in the Data Protection Legislation.

Infrastructure Key Infrastructure (or IKI) means the public key infrastructure established by the DCC for the purpose, among other things, of authenticating communications between:
(a) Parties and the OCA and DCA; and
(b) Parties and the DCC, where those Parties are required in accordance with this Code to provide files to the DCC that have been Digitally Signed using the Private Key associated with the Public Key that is contained within a File Signing Certificate.

Insolvency Type Event

means, in respect of a Party, that that Party:
(a) is unable to pay its debts as they fall due, or is deemed to be unable to pay its debts within the meaning of section 123 of the Insolvency Act 1986 (but as if the reference in such section to "£750" was replaced with "£10,000");
(b) calls a meeting for the purpose of passing a resolution for its winding-up, or such a resolution is passed;
(c) presents, or has presented in respect of it, a petition for a winding-up order;
(d) has an application to appoint an administrator made in respect of it, or a notice of intention to appoint an administrator is filed in respect of it;
(e) has an administrator, administrative receiver, or receiver appointed over all or a substantial part of its business, undertaking, property or assets;
(f) takes any steps in connection with proposing a company voluntary arrangement or a company voluntary arrangement is passed in relation to it; or
(g) suffers or undergoes any procedure analogous to any of those specified above, including in respect of a Party who is a natural person or in any jurisdiction outside the UK in which a Party is incorporated.

Installation End Date

has the meaning given to that expression in Section A3.12(b) (The Installation Validity Period).

Installation Start Date

has the meaning given to that expression in Section A3.12(a) (The Installation Validity Period).

Installation Validity Period

has the meaning given to that expression in Section A3.11 (The Installation Validity Period).

Instruction

means, in respect of a SMETS1 Device, a communication generated by the SMETS1 Service Provider or a DCO following receipt of a SMETS1 Service Request by the DCC that is designed to instruct the Device to execute the functionality necessary to permit the DCC to take the necessary Equivalent Steps.

Intellectual Property Rights

means patents, trade marks, trade names, service marks, rights in designs, copyright (including rights in computer software), logos, rights in internet domain names, and moral rights, database rights, rights in know-how, and other intellectual property rights (in each case, whether registered or unregistered or subject to an application for registration), and includes any and all rights or forms of protection having equivalent or similar effect anywhere in the world.

Interim Election

has the meaning given to that expression in Section C4.2 (Election of Elected Members).

Interoperability and Innovation Events

means the Testing Service described in Section H14.49 (Interoperability and Innovation Events).

Interoperability Checker Service

has the meaning given to that expression in Section H16.6 (Obligations of the DCC).

Interoperability Data

has the meaning given to that expression in Section H16.2 (The Responsibility of Supplier Parties).

Intimate Communications Hub Interface Specifications

means the specifications described as such and originally developed by the DCC pursuant to schedule 3 of the DCC Licence, as amended from time to time in accordance with Section H12.9 (Amendments to the ICHIS).

Inventory Enrolment and Decommissioning Procedures

means the SEC Subsidiary Document of that name set out as Appendix AC.

Invoice

has the meaning given to that expression in Section J1.2 (Invoicing of Charges).

Issue

in relation to:
(a) a Device Certificate or DCA Certificate, has the meaning given to that expression in Annex A of the Device Certificate Policy;
(b) an Organisation Certificate or OCA Certificate, has the meaning given to that expression in Annex A of the Organisation Certificate Policy;
(c) an IKI Certificate or ICA Certificate has the meaning given to that expression in the IKI Certificate Policy;
(d) a DCCKI Certificate (including any DCCKICA Certificate) has the meaning given to that expression in the DCCKI Certificate Policy.

Issuing DCA

has the meaning given to that expression in Annex A of the Device Certificate Policy.

Issuing DCA Certificate

has the meaning given to that expression in Annex A of the Device Certificate Policy.

Issuing ICA has the meaning given to that expression in the IKI Certificate Policy.

Issuing ICA Certificate has the meaning given to that expression in the IKI Certificate Policy.

Issuing OCA has the meaning given to that expression in Annex A of the Organisation Certificate Policy.

Issuing OCA Certificate has the meaning given to that expression in Annex A of the Organisation Certificate Policy.

Key Pair means a Private Key and its mathematically related Public Key, where the Public Key may be used to Check Cryptographic Protection in relation to a communication that has been Digitally Signed using the Private Key.

Known Remote Party has the meaning given to that expression in the GB Companion Specification.

Large Supplier Party means a Supplier Party that is not a Small Supplier Party.

Laws and Directives means any law (including the common law), statute, statutory instrument, regulation, instruction, direction, rule, condition or requirement (in each case) of any Competent Authority (or of any authorisation, licence, consent, permit or approval of any Competent Authority).

Lead Code means the Energy Code which the Cross Code Steering Group has designated as being the Lead Code for the purpose of progressing a variation that is likely to have an impact on any other Energy Codes.

Lead Code Modification means the variation to the Lead Code that gives rise to an associated Consequential Change.

Lead Supplier means, in respect of a Communications Hub:
(a) where there is only one Responsible Supplier for the Communications Hub Function which forms part of that Communications Hub, that Responsible Supplier; or
(b) where there is more than one Responsible Supplier for the

Communications Hub Function which forms part of that Communications Hub, the Import Supplier for the Communications Hub Function.

Letter of Credit means an unconditional irrevocable standby letter of credit in substantially the form set out in Schedule 6 from a bank with the Required Bank Rating which letter of credit has not been breached or disclaimed by the provider.

Liability includes any loss, liability, damages, costs (including legal costs), expenses and claims.

Local Command Services means the sending of Commands to a User via the DCC User Interface where the User has opted in the Service Request for the Command to be sent in that way.

Maintenance includes repair, replacement, upgrade or modification.

Maintenance End Date has the meaning given to that expression in Section A3.20(b) (The Maintenance Validity Period).

Maintenance Start Date has the meaning given to that expression in Section A3.20(a) (The Maintenance Validity Period).

Maintenance Validity Period has the meaning given to that expression in Section A3.19 (The Maintenance Validity Period) or (in the case of the DUIS) Section A3.36 (DCC User Interface Specification and Message Mapping Catalogue).

Major Incident means an Incident that is categorised as a major incident in accordance with the Service Management Standards, as further described in the Incident Management Policy.

Major Security Incident means, in relation to any System, any event which results, or was capable of resulting, in that System being Compromised to a material extent.

Malicious Software means any software program or code intended to destroy, interfere with, corrupt, or cause undesired effects on Data, software, files, programs or codes (whether or not its operation is immediate or delayed, and whether it is introduced wilfully, negligently or without knowledge of its existence).

Manufacturer means, in respect of any Device Model, the person:
(a) that manufactures some or all of the Devices of that Device Model; or
(b) on whose behalf some or all of those Devices are manufactured for onward sale or other provision.

Manufacturer Image has the meaning given to that expression in the GB Companion Specification.

MAP means Meter Asset Provider.

MAP/Manufacturer Reports means the reports provided by the DCC under Section H17 (MAP/Manufacturer Reports).

Market Participant Identifier has the meaning given to that expression in the Retail Energy Code.

MA-S Registry Entry means a publicly registered 36-bit identifier of that name issued by the Institute of Electrical and Electronics Engineers Standards Association.

Material Risk means, in respect of any Maintenance of the DCC Systems, that such Maintenance poses either: (a) a material risk of disruption; or (b) a risk of material disruption.

Maximum Credit Value has the meaning given to that expression in Section J3.8 (Party's Maximum Credit Value).

Mesh Communications Hub has the meaning given to that expression in the CH Support Materials.

Meter Asset Provider means, in respect of a Smart Meter, the entity that makes the Smart Meter available for use by Supplier Parties (and which is usually the owner of the Smart Meter).

Message has the meaning given to that expression in the GB Companion Specification.

Message Authentication Code has the meaning given to that expression in the GB Companion Specification (or, where used in the context of a communication not specified by the GB Companion Specification, the meaning associated with the relevant cryptographic algorithm used to generate it).

Message Code has the meaning given to that expression in the SMETS1 Supporting Requirements.

Message Mapping Catalogue means the SEC Subsidiary Document of that name set out in Appendix AF.

Meter Asset Manager has the meaning given to that expression in the UNC.

Meter Operator has the meaning given to the expression "Meter Operator Agent" in the BSC.

Metering Point has the meaning given to that expression in the REC.

Minimum Monthly Charge means, in respect of each Regulatory Year, £25.00, multiplied by the Consumer Prices Index for the October preceding the start of that Regulatory Year, divided by the Consumer Prices Index for October 2014. The relevant amount will be rounded to the nearest pound.

Minimum Service Level means, in respect of each Performance Measure, the number or percentage intended to represent the minimum level of performance for the activity which is the subject of the Performance Measure, as set out in:
(a) Section D11.3 (Code Performance Measures);
(b) Section H13.1 (Code Performance Measures);
(c) the Reported List of Service Provider Performance Measures; or
(d) Section L8.6 (Code Performance Measures).

Modification Proposal is the term applied to a Draft Proposal once the Panel has agreed it should be progressed further in accordance with Section D3.11 (Initial Consideration by the Panel).

Modification Register has the meaning given to that expression in Section D1.8 (Modification Register).

Modification Report has the meaning given to that expression in Section D7.1 (Modification Report).

Modification Report Consultation has the meaning given to that expression in Section D7.8 (Modification Report Consultation).

Monthly Service Metric has the meaning set out in the DCC User Interface Services Schedule.

Monthly Service Threshold has the meaning set out in the DCC User Interface Services Schedule.

MPAN means, in respect of a Smart Metering System (or Electricity Meter), the unique identifier (or each of the unique identifiers) allocated by the relevant Electricity Network Party to the Metering Point(s) at which the import or export of electricity is recorded by that Smart Metering System (or Electricity Meter).

MPRN means, in respect of a Smart Metering System (or Gas Meter), the Supply Meter Point Reference Number allocated by the relevant Gas Network Party to the Supply Meter Point at which the supply of gas is recorded by that Smart Metering System (or Gas Meter).

NCSC means the UK Government’s National Cyber Security Centre (or any successor organisation).

Network Enhancement Plan means a plan by the DCC to undertake works to improve SMETS2+ SM WAN connectivity for a cohort of Communications Hubs installed within a particular geographic area (in either the south Region or the central Region), where the DCC has obtained reasonable evidence to justify that the works are required in order to improve SM WAN connectivity.

Network Evolution Transition and Migration Approach Document (NETMAD) means the SEC Subsidiary Document set out in Appendix [TBC].

Network Party means a Party that is either an Electricity Network Party or a Gas Network Party.

Network Time has the meaning given to that expression in Section G2.45(a) (Network Time).

Never means a date-time used to denote the timing of an action that must never happen. For Service Requests, in accordance with DUIS, this date-time shall be 00:00:00 on 31st December 3000.

New Party means a Party that is a Party pursuant to an Accession Agreement.

Non-Critical Service Request means a Service Request which is not identified as critical in the DCC User Interface Services Schedule (or, in the case of Elective Communication Services, the relevant Bilateral Agreement).

Non-Critical Service Response means a Service Response in respect of a Non-Critical Service Request.

Non-Default Interest Rate means, for any day, the base lending rate of the Bank of England at 13.00 hours on that day.

Non-Device Service Request means a Service Request in respect of a Service identified as a non-device service in the DCC User Interface Services Schedule (or, in the case of Elective Communication Services, the relevant Bilateral Agreement).

Non-Domestic Premises means premises other than Domestic Premises.

Non-EPCL Device Model means a Device Model that appears on the Central Products List, but that does not appear within at least one entry on the SMETS1 Eligible Product Combinations List.

OCA Certificate has the meaning given to that expression in Annex A of the Organisation Certificate Policy.

On-Demand Services has the meaning given to that expression in Section H3.11 (Categories of Services).

OPR Exceptional Event means Force Majeure for which the DCC is the Affected Party and which occurs in relation to the matters which are subject to OPR Reporting.

OPR Reporting means reporting in respect of the operational performance regime under schedule 4 of the DCC Licence (the Operational Performance Regime).

Organisation Authority Revocation List (or Organisation ARL) has the meaning given to that expression in Annex A of the Organisation Certificate Policy.

Organisation Certificate has the meaning given to that expression in Annex A of the Organisation Certificate Policy.

Organisation Certificate Policy means the SEC Subsidiary Document of that name set out in Appendix B.

Organisation Certificate Revocation List (or Organisation CRL) has the meaning given to that expression in Annex A of the Organisation Certificate Policy.

Organisation Certification Authority (or OCA) has the meaning given to that expression in Annex A of the Organisation Certificate Policy.

Organisation Certification Practice Statement (or Organisation CPS) has the meaning given to that expression in Section L9.14 (the Organisation Certification Practice Statement).

Original Party means a Party that is a Party pursuant to the Framework Agreement.

OTA Header has the meaning given to that expression in the GB Companion Specification.

Other Enabling Services means the Services other than the Enrolment Services, the Communications Hub Services and the Communication Services.

Other SEC Party means a Party that is not the DCC, is not a Network Party, and is not a Supplier Party.

Other User means, for a Smart Metering System or a Device and any period of or point in time, a User that is not acting in the User Role of Import Supplier, Export Supplier, Gas Supplier, Electricity Distributor, Gas Transporter or Registered Supplier Agent (regardless of whether in fact that User is a Responsible Supplier or the Electricity Distributor or the Gas Transporter or the Registered Supplier Agent during that period of or at that point in time).

Panel means the body established as such in accordance with Section C2.1 (Establishment of the Panel).

Panel Chair has the meaning given to that expression in Section C3.1 (Composition of the Panel).

Panel Member has the meaning given to that expression in Section C3.1 (Composition of the Panel).

Panel Objectives has the meaning given to that expression in Section C2.2 (Panel Objectives).

Parent Company Guarantee means a guarantee in such form as the DCC may reasonably approve from an Affiliate of the User in question which guarantee has not been breached or disclaimed by the guarantor and has at least one month left until it expires. Where the guarantor is incorporated outside of the United Kingdom, the guarantee will only be validly given where supported by a legal opinion regarding capacity and enforceability in a form reasonably satisfactory to the DCC.

Parse and Correlate Software has the meaning given to that expression in Section H11.1 (Provision of Parse and Correlate Software).

Parse and Correlate Applicability Matrix has the meaning given to that expression in Section A3.39 (The Parse and Correlate Applicability Matrix).

Party means, from time to time, a person that has agreed to be bound by this Code (either pursuant to the Framework Agreement or an Accession Agreement), and (without prejudice to Section M8.14 (Consequences of Ceasing to be a Party)) that has not at that time ceased to be so bound in accordance with Section M8 (but excluding SECCo).

Party Category

means, as the context requires, one of the following categories:
(a) the Large Supplier Parties collectively;
(b) the Small Supplier Parties collectively;
(c) the Electricity Network Parties collectively;
(d) the Gas Network Parties collectively; and
(e) the Other SEC Parties collectively.

Party Data

has the meaning given to that expression in Section M5.10 (Party Data).

Party Details

means, in respect of each Party, the information relating to that Party and corresponding to the heads of information set out in the Application Form from time to time.

Party Signifier

means an identification number allocated to a Party (or SECCo) by the Code Administrator pursuant to Section B1.17 (Party Signifiers), which uniquely identifies that Party (or SECCo) under the Code.

Path 1 Modification

has the same meaning as “Authority-initiated Modification”.

Path 2 Modification

has the same meaning as “Authority Determined Modification.”

Path 3 Modification

has the same meaning as “Self-Governance Modification.”

Performance Indicators

means an indicator of service performance from time to time determined by the Panel under Section H13.5B (Performance Indicators), on which the DCC is to report but which does not constitute a Performance Measure.

Performance Measurement Methodology

means a documented methodology for establishing the performance against each Performance Measure, which may include sampling and/or test communications.

Performance Measurement Period

means, in respect of each Performance Measure, the applicable period over which the Service Level for that Performance Measure is to be measured, as set out in:
(a) Section D11.3 (Code Performance Measures);
(b) Section H13.1 (Code Performance Measures);
(c) the Reported List of Service Provider Performance Measures; or
(d) Section L8.6 (Code Performance Measures).

Performance Measures

means the Code Performance Measures and such Service Provider Performance Measures as are specified in the Reported List of Service Provider Performance Measures.

Permitted Communication Service

means, in respect of a User and a Smart Metering System (or a Device forming, or to form, part of that Smart Metering System):
(a) a service that results in the sending of a Command to a Device (other than the Communications Hub Function) for which the User is the Responsible Supplier (except where, were the Command to be sent as a Core Communication Service, it would be a Critical Command requiring another User's Digital Signature);
(b) a service that only results in the sending of a Command to a Device which is the same as a Command which results from a Service listed in the DCC User Interface Services Schedule for which that User is an Eligible User; or
(c) a service which the Panel has (on the application of the User) approved as a permitted communication service.

Personal Data

has the meaning given to that expression in the Data Protection Legislation.

Personnel Authentication Certificate

has the meaning given to that expression in Annex A of the DCCKI Certificate Policy.

Personnel Authentication Certificate Application

has the meaning given to that expression in Annex A of the DCCKI Certificate Policy.

Physical Device Type

means, in respect of a device, its type which may be only one of: a Communications Hub; a SMETS1 ESME; a Single Element Electricity Metering Equipment (as defined in the ESMETS); a Twin Element Electricity Metering Equipment (as defined in the ESMETS); a Polyphase Electricity Metering Equipment (as defined in the ESMETS), a Gas Smart Meter; a Pre-Payment Meter Interface Device; a HAN Connected Auxiliary Load Control Switch; an IHD; a Standalone Auxiliary Proportional Controller or a Type 2 Device (Other).

Planned Maintenance

means, in respect of a month, Maintenance of the DCC Systems planned prior to the start of that month which will disrupt or poses a Material Risk of disruption to the provision of the services described in a) and b) below (and, where it will disrupt, or poses a Material Risk of disruption to, the provision of these services in relation to Devices associated with Communications Hubs, at least 100,000 Communications Hubs are affected). Planned Maintenance shall be categorised as:
(a) High Impact Planned Maintenance where one or more of the following

is disrupted:

i. end-to-end communications between Users and Communications Hubs in either direction;
ii. install & commission activities; or
iii. previously scheduled SMETS1 migrations.

(b) Low Impact Planned Maintenance which will disrupt or poses a Material Risk of disruption to the provision of services, excluding those services set out in High Impact Planned Maintenance, and will not require changes to be made by Users except in cases where Service Improvements are being made to the SSI.

Point-to-Point Alt HAN Equipment has the meaning given to that expression in accordance with standard condition 55 of the Electricity Supply Licence (Smart Metering – The Alt HAN Arrangements) and standard condition 49 of the Gas Supply Licence (Smart Metering – The Alt HAN Arrangements).

Post Commissioning Information has the meaning given to that expression in the Inventory Enrolment and Decommissioning Procedures.

Power Outage & Restoration Alerts Delivery Management Document means the document established under Section H3.14B (Target Response Times) which contains the Target Response Times (and the methodology for reviewing and determining these times) for the Alerts which are subject to Section H3.14(i) or H3.14(j).

PPM Installation End Date has the meaning given to that expression in Section A3.14.

PPMID means a Prepayment Meter Interface Device.

PPMID Technical Specification (or **PPMIDTS)** means the part(s) of the document(s) set out in Schedule 9 identified as applying to 'Pre-Payment Meter Interface Devices'.

Pre-Command means a communication (other than a Service Response, DCC Alert or Device Alert) to be sent from the DCC to a User or to the CoS Party that includes a GBCS Payload and which has been Digitally Signed by the DCC in accordance with the DCC User Interface Specification.

Preliminary Assessment has the meaning given to that expression in Section H7.4 (Preliminary Assessment of Elective Communication Services).

Pre-Payment Consumer means an Energy Consumer at a premises for which the supply of energy is measured by a Smart Meter that is operating as a Pre-Payment Meter.

Pre-Payment Meter means an Energy Meter operating in a mode which requires a customer to pay charges in advance.

Pre-Payment Meter Interface Device means either a SMETS1 PPMID; or a device installed (or to be installed) at a premises, which:
(a) consists of the components or other apparatus identified in; and
(b) as a minimum, has the functional capability specified by and complies with the other requirements of,
a Version of the PPMID Technical Specification which was within its Installation Validity Period on the date on which the device was installed.

Principal User Security Obligations has the meaning given to that expression in Section G1.7 (Obligations on Users).

Principal Version in relation to:
(a) a Technical Specification, has the meaning given to that expression in Section A3.5(a) (Versions of the Technical Specifications); and
(b) the GBCS or CPA Security Characteristics, has the equivalent meaning, in accordance with and subject to the provisions of Section A3.27 (GB Companion Specification and CPA Security Characteristics).

Privacy Assessment means a Full Privacy Assessment, Random Sample Privacy Assessment or User Privacy Self-Assessment.

Privacy Assessment Report has the meaning given to that expression in Section I2.19 (The Privacy Assessment Report).

Privacy Assessment Response has the meaning given to that expression in Section I2.21 (The Privacy Assessment Response).

Privacy Controls Framework means the document of that name developed and maintained by the Panel in accordance with Section I2.15 (The Privacy Controls Framework).

Privacy Self-Assessment has the meaning given to that expression in Section I2.14 (Categories of Assessment).

Privacy Self-Assessment Report has the meaning given to that expression in Section I2.26 (The User Privacy Self-Assessment Report).

Private Key means the private part of an asymmetric Key Pair used for the purposes of public key encryption techniques

Privileged Person means a member of DCC Personnel who is authorised to carry out activities which involve access to resources, or Data held, on the DCC Total System and which are capable of being a means by which the DCC Total System, any User Systems, any RDP Systems or any Device are Compromised to a material extent.

Problem means the underlying cause of one or more Incidents, as further described in the Incident Management Policy.

Processing has the meaning given to that expression in the Data Protection Legislation (and “**Process**” and "**Processes**" shall be interpreted accordingly).

Product Recall or Technology Refresh has the meaning given to that expression in Section F9.6 (Categories of Responsibility).

Production Proving means the activities which the DCC is permitted to undertake by Section P (Production Proving).

Production Proving Devices has the meaning given to that expression in Section P1.4 (Production Proving Devices).

Production Proving Function means the DCC when undertaking Production Proving, and specifically those activities expressly stated in this Code to be undertaken by the Production Proving Function.

Production Proving MPXNs has the meaning given to that expression in Section P1.8 (Production Proving MPXNs).

Production Proving Registration Data has the meaning given to that expression in Section P1.11 (Production Proving Registration Data).

Production Proving Systems means the Systems used by the DCC in its capacity as the Production Proving Function.

Programme Assurance Policy has the meaning given to that expression in Section C2.3 (Panel Duties).

Proposed Solution means the variation under a Modification Proposal that is proposed and can be subsequently changed by the Proposer in accordance with Section D6.15 (Alternative Solutions).

Proposer has the meaning given to that expression in Section D1.3 (Persons Entitled to Submit Draft Proposals).

Prototype Communications Hub means a device that as closely achieves compliance with the CHTS as is reasonably practicable from time to time, which is provided (or to be provided) for the purpose of testing as described in Section F10 (Test Communications Hubs).

Public Key means the public part of an asymmetric Key Pair used for the purposes of public key encryption techniques.

Random Sample Privacy Assessment has the meaning given to that expression in Section I2.13 (Categories of Assessment).

RDP means Registration Data Provider.

RDP Entry Process Tests has the meaning given to that expression in Section E4.2 (RDP Entry Process Tests).

RDP ID means, in respect of an RDP acting in its capacity as such (including a Network Party where it is deemed to have nominated itself for that role), one of the unique identification numbers accepted by the DCC in respect of that RDP under Section E2.16 (Security Obligations and RDP IDs).

RDP Signifier

means an identification number allocated to an RDP by the Code Administrator pursuant to Section B1.19 (RDP Signifiers), which uniquely identifies that RDP under the Code.

RDP Systems

means any Systems:

(a) which are operated by or on behalf of an Electricity Distributor or Gas Transporter responsible for providing (or procuring the provision of) Registration Data in respect of a particular MPAN or MPRN; and

(b) which are used in whole or in part for generating Data for communication to the OCA, ICA or DCCKICA, or receiving Data from the OCA, ICA or DCCKICA (including any Systems which store or use Secret Key Material for such purposes),

and any other Systems from which the Systems described in paragraphs (a) and (b) are not Separated.

REC

means the Retail Energy Code maintained pursuant to Condition 11B of the Electricity Supply Licences and Condition 11 of the Gas Supply Licences.

REC Code Manager

has the meaning given to the expression "Code Manager" in the REC.

Recoverable Costs

has the meaning given to that expression in Section C8.2 (SEC Costs and Expenses).

Recovery Certificate

has the meaning given to that expression in Section L10.30(d)(ii) (Definitions).

Recovery Costs

has the meaning given to that expression in Section L10.17 (Recovery Costs).

Recovery Event

has the meaning given to that expression in Section L10.14 (Recovery Events).

Recovery Key Pair

has the meaning given to that expression in Section L10.30(d) (Definitions).

Recovery Private Key

has the meaning given to that expression in Section L10.30(d)(i) (Definitions).

Refinement Process has the meaning given to that expression in Section D6 (Refinement Process).

Region means each of the regions of Great Britain that are subject to different DCC Service Provider Contracts, and the region into which a premises (or future potential premises) falls shall be:

(a) identified insofar as reasonably practicable in a document published by the DCC (or the Panel on behalf of the DCC) from time to time; or

(b) where a premises (or future potential premises) is not so identified, confirmed by the DCC on application of any Party or in response to the resolution of an Incident regarding the fact that a premises (or future potential premises) is not so identified,

and once a premises has been identified by the DCC as being in a particular region, the DCC shall not identify that premises as being in a different region (unless agreed by the Supplier Party or Supplier Parties Registered for the MPAN and/or MPRN at the premises and the Network Party or Network Parties for the network(s) to which the premises is, or is intended to be, connected).

Registered means the Registered Supplier, as defined in the REC (and "**Registration**" shall be interpreted accordingly).

Registered Supplier Agent means, for a Smart Metering System or a Device and any period of or point in time, the User that is:

(a) in the case of electricity, appointed as the Meter Operator in respect of the MPAN relating to that Smart Metering System or Device; or

(b) in the case of gas, appointed as the Meter Asset Manager in respect of the MPRN relating to that Smart Metering System or Device,

(in either case) during that period of or at that point in time.

Registration Authority means the DCC, acting in its capacity as such for the purposes of (and in accordance with the meaning given to that expression in any) the Certificate Policies.

Registration Data has the meaning given to that expression in Section E1 (Reliance on Registration Data).

Registration Data Interface means the communications interface designed to allow the communications referred to in Section E (Registration Data) to be sent between the DCC and the Registration Data Providers.

Registration Data Interface Code of Connection

means the SEC Subsidiary Document of that name set out in Appendix Y.

Registration Data Interface Documents

means the Registration Data Interface Code of Connection and Registration Data Interface Specification.

Registration Data Interface Specification

means the SEC Subsidiary Document of that name set out in Appendix X.

Registration Data Provider

means, in respect of each Network Party, the person nominated as such in writing to the DCC from time to time by that Network Party, on the basis that more than one Party may specify the same Registration Data Provider, and that the Network Party shall be deemed to have so nominated itself in the absence of any other nomination.

Regulatory Year

means a period of twelve months beginning at the start of 1 April in any calendar year and ending at the end of 31 March in the next following calendar year.

Related Person

means, in relation to an individual, that individual’s spouse, civil partner, parent, grandparent, sibling, child, grandchild or other immediate family member; any partner with whom that individual is in partnership; that individual’s employer; any Affiliate of such employer; any person by whom that individual was employed in the previous 12 months; and any company (or Affiliate of a company) in respect of which that individual (individually or collectively with any member of his immediate family) controls more than 20% of the voting rights.

Release Management

means the process adopted for planning, scheduling and controlling the build, test and deployment of releases of IT updates, procedures and processes.

Relevant Device

has the meaning given to that expression in Section L10.30(a) (Definitions).

Relevant Instruments

means:
(a) the Electricity Act and the Gas Act;
(b) the Data Protection Legislation;
(c) the Energy Licences; and
(d) the Energy Codes.

Relevant Private Key has the meaning given to that expression in Section L10.30(c) (Definitions).

Relevant Subscriber has the meaning given to that expression in Section L10.30(b).

Relevant Technical Specification Means:

a. in relation to an Electricity Smart Meter, Gas Smart Meter, HAN Connected Auxiliary Load Control Switch, IHD, Pre-Payment Meter Interface Device, or Standalone Auxiliary Proportional Controller, the ESMETS, GSMETS, HCALCSTS, IHDTS, PPMIDTS or SAPCTS respectively;
b. in relation to a Communications Hub Function, the CHTS (but excluding those provisions that are described as applying only to "Gas Proxy Functions"); or
c. in relation to a Gas Proxy Function, the CHTS (but only those provisions that are described as applying to "Gas Proxy Functions").

Relying Party means a person who, pursuant to the Code, receives and relies upon a Certificate.

Relying Party Obligations means the provisions in respect of Relying Parties set out at Section L12 of the Code (the Relying Party Obligations).

Remote Party has the meaning given to that expression in GBCS.

Remote Party Role has the meaning given to that expression, and comprises the values allowed for the ASN.1 type RemotePartyRole identified, in the GB Companion Specification, and additionally comprises the values set out in Table 1 in Annex A to Section L (Smart Metering Key Infrastructure and DCC Key Infrastructure).

Remote Party Role Code means the integer value for the Remote Party Role specified in the GB Companion Specification or Table 1 in Annex A to Section L (Smart Metering Key Infrastructure and DCC Key Infrastructure), as applicable.

Replacement Meter means an Energy Meter that replaces an Energy Meter previously installed at the same premises.

Replay

has the meaning given to that expression in the SMETS1 Supporting Requirements.

Report Phase

has the meaning given to that expression in Section D7.1 (Modification Report).

Reported List of Service Provider Performance Measures

means the document which:
(a) is initially provided to Parties, the Panel and the Authority by the Secretary of State, bears the title 'Reported List of Service Provider Performance Measures' and identifies itself as being produced for the purposes of Section H13 (Performance Standards and Reporting); and
(b) specifies a number of Service Provider Performance Measures together (in each case) with the applicable Service Level Requirement, Target Service Level, Minimum Service Level and Performance Measurement Period,
as it may be modified from time to time in accordance with Section H13.2 (Service Provider Performance Measures).

Required Bank Rating

means that a person has one or more long-term Recognised Credit Ratings of at least (based, where the person has more than one such rating, on the lower of the ratings):
(a) “A-” by Standard & Poor’s Financial Services LLC;
(b) “A3” by Moody’s Investors Services Inc; and/or
(c) “A-” by Fitch Ratings Limited; and/or
(d) “A(low)” by DBRS Ratings Limited.

Response

for SMETS2+ Devices, has the meaning given to that expression in the GB Companion Specification; and otherwise, it shall mean a Service Response or a Pre-Command as the context implies.

Responsible Supplier

means, in respect of a Smart Metering System (or any Device forming, or intended to form, part of a Smart Metering System) which relates to:
(a) an MPAN, the Import Supplier for that Smart Metering System; and/or
(b) an MPRN, the Gas Supplier for that Smart Metering System.

Restricted Communication Service

means, in respect of any User requesting an Elective Communication Service, a service which is not a Permitted Communication Service.

RF Noise Testing

means the Testing Service described in Section H14.46 (Radio Frequency Noise Testing).

Risk Treatment Plan has the meaning given to that expression in Section G7.19(e) (Duties and Powers of the Security Sub-Committee).

Root DCA has the meaning given to that expression in Annex A of the Device Certificate Policy.

Root DCA Certificate has the meaning given to that expression in Annex A of the Device Certificate Policy.

Root DCCKICA Certificate has the meaning given to that expression in the DCCKI Certificate Policy

Root ICA has the meaning given to that expression in the IKI Certificate Policy.

Root ICA Certificate has the meaning given to that expression in the IKI Certificate Policy.

Root OCA has the meaning given to that expression in Annex A of the Organisation Certificate Policy.

Root OCA Certificate has the meaning given to that expression in Annex A of the Organisation Certificate Policy.

SAPC means a Standalone Auxiliary Proportional Controller.

SAPC Technical Specification (or SAPCTS) means the part(s) of the document(s) set out in Schedule 9 identified as applying to 'Standalone Auxiliary Proportional Controllers'.

Scheduled Election has the meaning given to that expression in Section C4.2 (Election of the Elected Members).

Scheduled Services has the meaning given to that expression in Section H3.11 (Categories of Services).

SEC Arrangements has the meaning given to that expression in the DCC Licence.

SEC Materials has the meaning given to that expression in Section M5.1 (SEC Materials).

SEC Objectives means, in respect of the Charging Methodology only, the Charging Objectives and, in all other cases, the General SEC Objectives.

SEC Release means a package of one or more approved Modification Proposals which is implemented in accordance with the SEC Release Management Policy.

SEC Release Implementation Document means a document established under Section D10.12 (SEC Release Implementation Document) and which contains the information listed in Section D10.13.

SEC Release Management Policy means the document established under Section D10.7 (SEC Release Management Policy) and which contains the information listed in Section D10.8.

SEC Release Testing Approach Document means a document established under Section D10.18 (SEC Release Testing Approach Document) and which contains the information listed in Section D10.19 in relation to the testing to be undertaken by the DCC with regards to a SEC Release.

SEC Variation Testing Approach Documents means the SEC Subsidiary Documents set out in Appendix AJ, Appendix AK, Appendix AN, Appendix AQ and Appendix AR.

SECCo has the meaning given to that expression in Schedule 4.

Secret Key Material means any Private Key, Shared Secret, Symmetric Key, SMETS1 Symmetric Key or other functionally equivalent cryptographic material (and any associated input parameter) that is generated and maintained by a Party or RDP for the purposes of complying with its obligations under, or in relation to, this Code, but excluding:
(a) any such material (and associated input parameters) to the extent that it is maintained on Devices;
(b) any Digital Signature; and
(c) any output of a Cryptographic Hash Function operating on an input communication.

Secretariat has the meaning given to that expression in Section C7.6 (Secretariat).

Secretary of State has the meaning given to that expression in the Interpretation Act 1978.

Secure has the meaning given to that expression in Section G3.28(a) (SMETS1 Smart Metering Systems).

Security Check means the vetting of personnel, carried out to a level that is identified by that name, under and in accordance with the HMG National Security Vetting Procedures.

Security Controls Framework has the meaning given to that expression in Section G7.19(a) (Duties and Powers of the Security Sub-Committee).

Security Obligations and Assurance Arrangements means:
(a) in the case of the DCC Total System, those requirements set out in Sections G2, G4 to G7 and G9;
(b) in the case of User Systems, those requirements set out in Sections G3 to G8;
(c) in the case of Smart Metering Systems comprising SMETS2+ Devices, those requirements set out in:
(i) the Commercial Product Assurance Security Characteristics (as defined in the GB Companion Specification); and
(ii) the provisions of Sections G3 (System Security: Obligations on Users) to G8 (User Security Assurance) which are applicable to such Smart Metering Systems;
(d) in the case of SMETS1 Smart Metering Systems:
(i) those security requirements set out in (as applicable) the ESMETS, the GSMETS and the IHDTS with a Principal Version number of 1; and
(ii) those requirements set out in the provisions of Sections G3 to G8 which are applicable to such Smart Metering Systems; and
(e) in the case of RDP Systems, those requirements set out in Section E2.14 (Security Obligations).

Security Requirements means a document that:
(a) identifies the security controls that are considered appropriate to mitigate the security risks relating to the End-to-End Smart Metering System; and
(b) indicates those provisions having effect (or being proposed to have effect) in or under the Security Obligations and Assurance Arrangements or any Energy Licences which require that such security controls are established and maintained.

Security Risk Assessment means a document that identifies, analyses and evaluates the security risks which relate to the End-to-End Smart Metering System.

Security Sub-Committee means the Sub-Committee established pursuant to Section G7 (Security Sub-Committee).

Security Sub-Committee Guidance means guidance in respect of the security of any System, updated from time to time by the Security Sub-Committee.

Security Sub-Committee (Network) Members has the meaning given to that expression in Section G7.8 (Membership of the Security Sub-Committee).

Security Sub-Committee (Other User) Member has the meaning given to that expression in Section G7.10 (Membership of the Security Sub-Committee)

Security Sub-Committee (Shared Resource Provider Member) has the meaning given to that expression in Section G7.12 (Membership of the Security Sub-Committee)

Security Sub-Committee (Supplier) Members has the meaning given to that expression in Section G7.6 (Membership of the Security Sub-Committee).

Security Sub-Committee Chair has the meaning given to that expression in Section G7.5 (Membership of the Security Sub-Committee).

Security Sub-Committee Member has the meaning given to that expression in Section G7.3 (Membership of the Security Sub-Committee).

Self-Governance Modification has the meaning given to that expression in Section D2.7 (Self-Governance Modifications).

Self-Service Interface has the meaning given to that expression in Section H8.15 (Self-Service Interface).

Self-Service Interface Code of Connection

means the SEC Subsidiary Document of that name set out in Appendix AI.

Self-Service Interface Access Control Specification

means the SEC Subsidiary Document of that name set out in Appendix AH.

Separate

means, in relation to any System, software or firmware, to establish controls which are appropriately designed to ensure that no communication may take place between it and any other System, software or firmware (as the case may be) except to the extent that such communication is for a necessary purpose having regard to the intended operation of the System, software or firmware (and "**Separated**" and "**Separation**" are to be interpreted accordingly).

Sequenced Services

has the meaning given to that expression in Section H3.13 (Sequenced Services).

Service Desk

has the meaning given to that expression in Section H8.19 (Service Desk).

Service Level

means, in respect of each Performance Measure and each Performance Measurement Period:

(a) where that Performance Measure relates to an activity that is performed on a number of separate occasions:

(i) the number of occasions during the Performance Measurement Period on which that activity was performed in accordance with the relevant Service Level Requirement,

expressed as a percentage of, or a number in relation to:

(ii) the total number of occasions during the Performance Measurement Period on which that activity was performed;

(b) where that Performance Measure relates to an activity that is performed over a period of time:

(i) the period of time during the Performance Measurement Period on which that activity was performed, expressed as a percentage of:

(ii) the period of time during the Performance Measurement Period on which that activity would have been performed if it had been performed in accordance with the relevant Service Level Requirement,

provided that in each case the DCC may establish the Service Level for a Performance Measure in accordance with the Performance Measurement Methodology.

Service Level Requirements

means:

(a) in respect of each Code Performance Measure, the Target Response Time, Target Resolution Time or Target Availability Time (applicable in accordance with the table at Section D11.3 (Code Performance Measures), at Section H13.1 (Code Performance Measures) or at Section L8.6 (Code Performance Measures)); or

(b) in respect of each Service Provider Performance Measure, the standard to which the relevant DCC Service Provider is obliged by its DCC Service Provider Contract to perform the activity that is the subject of the Service Provider Performance Measure.

Service Management Service Request

means a query raised by a Party via the Self-Service Interface and/or the Service Desk.

Service Management Standards

means the Information Technology Infrastructure Library (ITIL®) standards for IT services management, as issued and updated by the Cabinet Office from time to time.

Service Provider Performance Measures

means the performance measures (however described and from time to time) for each DCC Service Provider under each DCC Service Provider Contract.

Service Reference Variant

means a reference assigned to a Service Request in accordance with the DCC User Interface Specification.

Service Request

means a request for one of the Services listed in the DCC User Interface Services Schedule (or, in the case of Elective Communication Services, provided for in the relevant Bilateral Agreement).

Service Request Processing Document

means the SEC Subsidiary Document of that name set out in Appendix AB.

Service Response

means, in respect of a Service Request sent by a User, one or more communications in response to that Service Request from the DCC to the User (not being a Pre-Command).

Services

means the services provided, or to be provided, by the DCC pursuant to Sections F5 (Communications Hub Forecasts and Orders) to F10 (Test Communications Hubs), Section H (DCC Services), Section L (Smart Metering Key Infrastructure and DCC Key Infrastructure) or Section N6 (Transition and Migration Approach Document), including pursuant to Bilateral Agreements.

Services FM means, in respect of any Services, the occurrence of any of the following:
(a) war, civil war, riot, civil commotion or armed conflict;
(B) terrorism (being the use or threat of action designed to influence the government or intimidate the public or for the purpose of advancing a political, religious or ideological cause and which involves serious violence against a person or serious damage to property, endangers a person's life, creates a serious risk to the public or is designed to seriously interfere with or disrupt an electronic system);
(c) nuclear, chemical or biological contamination;
(d) earthquakes, fire, storm damage or severe flooding (if in each case it affects a significant geographical area); and/or
(e) any blockade or embargo (if in each case it affects a significant geographical area).

Services IPR has the meaning given to that expression in Section M5.14 (Services IPR).

Shared Resource Provider has the meaning given to that expression in Section G10.2 (Meaning of Shared Resources).

Shared Resource User has the meaning given to that expression in Section G10.7 (Additional Obligations following User Security Assessments).

Shared Resources has the meaning given to that expression in Section G10.1 (Meaning of Shared Resources).

Shared Secret means a parameter that is (or may be) derived from a Private Key and a Public Key which are not from the same Key Pair in accordance with the GB Companion Specification.

Shared Solution Alt HAN Equipment has the meaning given to that expression in accordance with standard condition 55 of the Electricity Supply Licence (Smart Metering – The Alt HAN Arrangements) and standard condition 49 of the Gas Supply Licence (Smart Metering – The Alt HAN Arrangements).

Signed Pre-Command means a communication containing the Digitally Signed GBCS Payload of a Pre-Command that has been Digitally Signed by a User or the CoS Party.

Significant Code Review

means a review of one or more matters by the Authority which the Authority considers is:
(a) related to this Code (whether on its own or together with other Energy Codes); and
(b) likely to be of significance in relation to the Authority's principal objective and/or general duties (as set out in section 3A of the Electricity Act and section 4AA of the Gas Act), and statutory functions,
and concerning which the Authority has issued a notice that the review will constitute a significant code review.

Significant Code Review Phase

means, in respect of each Significant Code Review, the period from the date on which the Authority issues the notice stating that the matter is to constitute a Significant Code Review (including where the Authority issues a direction under Section D5.7 (Significant Code Review: Backstop Direction) or proposes an Authority-Led Variation by issuing a direction under Section D9A.2 (Authority Power to Develop a Proposed Variation)), and ending on the earlier of:
(a) the date on which the Authority, or DCC at the direction of the Authority, submits a Draft Proposal in respect of any variations arising out of a Significant Code Review;
(b) where the Authority has proposed an Authority-Led Variation, the date on which the Authority makes a decision in accordance with Section D9A.11 (Authority Decision);
(c) the date on which the Authority issues a conclusion that no modification is required to this Code as a result of the Significant Code Review; or
(d) the date 28 days after the date on which the Authority issues its conclusion document in respect of the Significant Code Review.

SIMCH Aerial

means an aerial and any other equipment required to enable a Special Installation Mesh Communications Hub to connect to the SMETS2+ SM WAN.

SM WAN

means the SMETS1 SM WAN or the SMETS2+ SM WAN.

SM WAN Coverage Database

means the information made available via the Self-Service Interface pursuant to Section H8.16(f) (and which is also available via the CH Ordering System).

Small Supplier Party

means a Supplier Party which, at the time at which it is necessary to assess the status of the Party, supplies electricity and/or gas to fewer than 250,000 (two hundred and fifty thousand) Domestic Premises.

Smart Card Token has the meaning given to that expression in Annex A of the DCCKI Certificate Policy.

Smart Meter means either an Electricity Smart Meter or a Gas Smart Meter (as the context requires).

Smart Meter Device Assurance Sub-Committee means the Sub-Committee established under Section F12 (Smart Meter Device Assurance Sub-Committee).

Smart Metering Equipment Technical Specifications (SMETS) shall be interpreted in accordance with the provisions of Section A2.12.

Smart Metering Inventory means an electronic database of Devices which records (as a minimum) the following information in respect of each Device:
(a) its Device Type;
(b) its Device ID;
(c) its Device Model (provided that no firmware version is needed for Type 2 Devices);
(d) for Devices other than Type 2 Devices, its SMI Status, and the date from which that status has applied;
(e) for Devices other than Type 2 Devices, its SMI Status history;
(f) where it is a Smart Meter which has been installed, the related MPAN or MPRN and the Communications Hub Function with which that Smart Meter is associated; and
(g) where it is a Device (other than a Smart Meter or a Communications Hub Function), the Smart Meter or Gas Proxy Function with which that Device is associated.

Smart Metering Key Infrastructure (or SMKI) means the public key infrastructure established by DCC for the purpose, among other things, of providing secure communications between Devices and Users.

Smart Metering System means either:
(a) an Electricity Smart Meter, together with the Communications Hub Function with which it is Associated, together with any SAPC or Additional Electricity Smart Meter joined to that Communications Hub Function, together with the Type 1 Devices (if any) that may from time to time be Associated with that Electricity Smart Meter; or
(b) a Gas Smart Meter together with the Communications Hub Function with which it is Associated and an Associated Gas Proxy Function, together

with the Type 1 Devices (if any) that may from time to time be Associated with that Gas Proxy Function.

Smart Mode has the meaning given to that expression at Section H16.15 (Definition).

SMDA Sub-Committee means the Smart Meter Device Assurance Sub-Committee.

SMETS1 means each composite document set out in Schedule 9 which includes within it an ESMETS, a GSMETS and an IHDTS with a Principal Version number of 1.

SMETS1 Alert has the meaning given to that expression in the DCC User Interface Specification.

SMETS1 CH means a physical device comprising a SMETS1 CHF and a SMETS1 GPF.

SMETS1 CHF means that part of a SMETS1 ESMS or SMETS1 GSMS which incorporates the wide area network interface and controls which Devices can communicate via the associated home area network interface.

SMETS1 Critical Service Request means a Critical Service Request which is targeted at a SMETS1 Device and is a SMETS1 Service Request.

SMETS1 Cryptographic Key Management Policy means any SEC Subsidiary Document of that name set out in Appendix AT, which is originally to be developed pursuant to Section L14.7 (The SMETS1 Cryptographic Key Management Policy: Document Development) and Section L14.8 (Document Development: Process).

SMETS1 CSP System has the meaning given to that expression at Section G1.11 (The SMETS1 CSP System).

SMETS1 Device means one of the following: (a) a SMETS1 ESME; (b) a SMETS1 GSME; (c) a SMETS1 CHF; (d) a SMETS1 GPF; (e) a SMETS1 PPMID; (f) a SMETS1 IHD; and (g) any other device operating on a home area network created by a SMETS1 CHF.

SMETS1 Device Model means the Device Model of a Device which complies with the requirements of SMETS1 (or which, in combination with other Devices, complies with the requirements of SMETS1).

SMETS1 Eligible Product Combinations has the meaning given to that expression in Section F2.10A (SMETS1 Lists).

SMETS1 ESME means that part of a SMETS1 ESMS that is not a SMETS1 CH.

SMETS1 ESMS has the meaning given to the expression 'ESMS' in SMETS1.

SMETS1 Future Dated Critical Service Request means a SMETS1 Critical Service Request which contains an execution date-time which is in the future according to the DCC's time.

SMETS1 GPF means that part of a SMETS1 GSMS that is not a SMETS1 CHF and is powered by mains electricity. For the avoidance of doubt, a SMETS1 GPF excludes any SMETS1 GSME.

SMETS1 GSME means that part of a SMETS1 GSMS that is not a SMETS1 CH.

SMETS1 GSMS has the meaning given to the expression 'GSMS' in SMETS1.

SMETS1 IHD has the meaning given to the expression 'IHD' in SMETS1.

SMETS1 Installation means a SMETS1 CHF installed in respect of an Energy Consumer's premises, the SMETS1 GPF which is part of the same SMETS1 CH, the SMETS1 ESME with which the SMETS1 CHF can communicate, and the set of other Devices (if any) which are authorised to communicate over the HAN to which the CHF controls access. The set of other Devices within a SMETS1 Installation shall include at most one SMETS1 GSME, at most one SMETS1 PPMID, at most one SMETS1 IHD and at most one SMETS1 CAD.

SMETS1 Pending Product Combinations Tests has the meaning given to that expression in Section H14.36A (SMETS1 Pending Product Combinations Tests).

SMETS1 Pending Product Combinations has the meaning given to that expression in Section F2.10A (SMETS1 Lists).

SMETS1 PPMID means a SMETS1 IHD that is capable of upgrading its Firmware in response to an Instruction sent over the SMETS1 SM WAN.

SMETS1 Response has the meaning given to that expression in the DCC User Interface Specification.

SMETS1 Service Provider means the DCC when carrying out the role and activities ascribed to a SMETS1 Service Provider in this Code; and where the DCC relies on the services of more than one DCC Service Provider for the purposes of carrying out that role and those activities, it shall be treated as being a separate SMETS1 Service Provider to the extent of its reliance on the services of each such DCC Service Provider.

SMETS1 Service Provider PKI (or S1SPKI) means any public key infrastructure established (or to be established) for the purpose, among other things, of providing secure communications between the DCC and SMETS1 Devices.

SMETS1 Service Request has the meaning given to that expression in the DCC User Interface Specification.

SMETS1 Smart Metering System means a Smart Metering System comprising SMETS1 Devices.

SMETS1 SMS means a SMETS1 Smart Metering System.

SMETS1 SMSO means a smart meter system operator that provides (or used to provide) some or all of the data and/or communications services in respect of SMETS1 Devices.

SMETS1 SM WAN means the means by which the DCC sends, receives and conveys communications to and from some or all SMETS1 CHFs (which may differ between SMETS1 CHFs).

SMETS1 Supported Service Request has the meaning given to that expression in the DCC User Interface Specification.

SMETS1 Supporting Requirements means the SEC Subsidiary Document set out in Appendix AM.

SMETS1 Symmetric Key means an Authentication Key or a symmetric key which is in either case used to process communications with SMETS1 Devices.

SMETS1 Symmetric Key Arrangement means any arrangement that is established (or is to be established) for the purpose, among other things, of providing secure communications between the DCC and SMETS1 Devices by means of using SMETS1 Symmetric Keys.

SMETS2+ Communications Hub means a Communications Hub which is not a SMETS1 CH.

SMETS2+ Device means a Device that:

a. consists of the components or other apparatus identified in; and
b. as a minimum, has the functional capability specified by and complies with the other requirements of, a Relevant Technical Specification (and, where applicable, the part(s) of the Relevant Technical Specification relevant to the Physical Device Type in question) in a Version of the Relevant Technical Specification which was within its Installation Validity Period on the date on which the Device was installed and which has (or had) a Principal Version that is 2 or higher.

SMETS2+ Device Model means the Device Model of a Device which complies with the requirements of SMETS2+ (or which, in combination with other Devices, complies with the requirements of SMETS2+).

SMETS2+ SM WAN means the means by which the DCC sends, receives and conveys communications to and from SMETS2+ Communications Hub Functions (which may differ from Region to Region).

S1SP means the SMETS1 Service Provider.

S1SP Alert

has the meaning given to that expression in the DCC User Interface Specification.

S1SPKI Certificate Policy (or S1SPKI CP)

means any SEC Subsidiary Document of that name set out in Appendices AP1 or AP2, which is originally to be developed pursuant to Section L14.5 (The S1SPKI Certificate Policies: Document Development) and Section L14.8 (Document Development: Process).

S1SPKI Certification Practice Statement (or S1SPKI CPS)

has the meaning given to that expression in Section L14.9 (The S1SPKI Certification Practice Statement).

S1SPKI Registration Authority Policies and Procedures (or S1SPKI RAPP)

means any SEC Subsidiary Document of that name set out in Appendix [TBC] or the section of the associated S1SPKI Certificate Policy identified as being the S1SPKI RAPP for that S1SPKI Certificate Policy, which is originally to be developed pursuant to Section L14.6 (The S1SPKI Registration Authority Policies and Procedures: Document Development) and Section L14.8 (Document Development: Process).

S1SPKM Compliance Policy

means the SEC Subsidiary Document of that name set out in Appendix AO.

S1SPKM Document Set

has the meaning given to that expression in Section L14.3 (The S1SPKM Document Set).

S1SPKM SEC Documents

has the meaning given to that expression in Section L.14.4 (The S1SPKM SEC Documents).

SMI Status

means the status indicator of each Device recorded within the Smart Metering Inventory, which indicator may (as a minimum) be set to any one of the following:
(a) ‘pending’, indicating that the Device has not yet been Commissioned;
(b) ‘installed not commissioned’, indicating that the Device is ready to be Commissioned, but has not yet been Commissioned;
(c) ‘commissioned’, indicating that the Device has been Commissioned;
(d) ‘decommissioned’, indicating that the Device has been Decommissioned;
(e) ‘suspended’, indicating that the Device has been Suspended;
(f) ‘whitelisted’, indicating that a Device has been added to the Device Log of a Communications Hub Function but that communications between the Device and the Communications Hub Function may not yet have been established;
(g) ‘recovery’, indicating that the processing of communications destined

for the Device has been disabled (other than for communications originated by the DCC) in accordance with the SMKI Recovery Procedure; or
(h) ‘recovered’, indicating that the Data comprising the Device Security Credentials have successfully been updated using Data from one or more OCA Certificates and/or Organisation Certificates for which DCC is the Subscriber as further described in the SMKI Recovery Procedure.

SMKI and Repository Entry Process Tests

means the tests described in Section H14.22 (SMKI and Repository Entry Process Tests).

SMKI and Repository Test Scenario Document

means the SEC Subsidiary Document of that name set out in Appendix K.

SMKI Code of Connection

means the SEC Subsidiary Document of that name set out in Appendix N, which:
(a) has the purpose described in Section L4.5 (SMKI Code of Connection); and
(b) is originally to be developed pursuant to Sections L4.6 to L4.7 (SMKI Interface Document Development).

SMKI Compliance Policy

means the SEC Subsidiary Document of that name set out in Appendix C.

SMKI Document Set

has the meaning given to that expression in Section L9.3 (the SMKI Document Set).

SMKI Independent Assurance Scheme

has the meaning given to that expression in Part 2.1 of the SMKI Compliance Policy (DCC: Duty to Submit to an SMKI Independent Assurance Scheme).

SMKI Interface Design Specification

means the SEC Subsidiary Document of that name set out in Appendix M, which:
(a) has the purpose described in Section L4.4 (SMKI Interface Design Specification); and
(b) is originally to be developed pursuant to Sections L4.6 to L4.7 (SMKI Interface Document Development).

SMKI Participants

means the DCC (acting in its capacity as the provider of the SMKI Services), all Authorised Subscribers and all Relying Parties.

SMKI PMA means the Sub-Committee of that name established pursuant to Section L1 (SMKI Policy Management Authority).

SMKI PMA (Network) Member has the meaning given to that expression in Section L1.8 (Membership of the SMKI PMA).

SMKI PMA (Supplier) Members has the meaning given to that expression in Section L1.6 (Membership of the SMKI PMA).

SMKI PMA Chair has the meaning given to that expression in Section L1.5 (Membership of the SMKI PMA).

SMKI PMA Guidance means guidance in respect of the SMKI Document Set, updated from time to time by the SMKI PMA.

SMKI PMA Member has the meaning given to that expression in Section L1.3 (Membership of the SMKI PMA).

SMKI Recovery Key Guidance has the meaning given to that expression in Section L10.9 (The SMKI Recovery Key Guidance).

SMKI Recovery Procedure means the SEC Subsidiary Document of that name set out in Appendix L, which:

(a) has the purpose described in Section L10.1 (The SMKI Recovery Procedure); and

(b) is originally to be developed pursuant to Sections L10.7 to L10.8 (SMKI Recovery Procedure: Document Development).

SMKI Registration Authority Policies and Procedures (or SMKI RAPP) means the SEC Subsidiary Document of that name set out in Appendix D, which is originally to be developed pursuant to Sections L9.5 to L9.6 (the Registration Authority Policies and Procedures: Document Development).

SMKI Repository has the meaning given to that expression in Section L5.1 (the SMKI Repository).

SMKI Repository Code of Connection means the SEC Subsidiary Document of that name set out in Appendix P, which:

(a) has the purpose described in Section L6.5 (SMKI Repository Code of Connection); and
(b) is originally to be developed pursuant to Sections L6.6 to L6.7 (SMKI Repository Interface Document Development).

SMKI Repository Interface has the meaning given to that expression in Section L6.3 (the SMKI Repository Interface).

SMKI Repository Interface Design Specification means the SEC Subsidiary Document of that name set out in Appendix O, which
(a) has the purpose described in Section L6.4 (SMKI Repository Interface Design Specification); and
(b) is originally to be developed pursuant to Sections L6.6 to L6.7 (SMKI Repository Interface Document Development).

SMKI Repository Service has the meaning given to that expression in Section L5.2 (the SMKI Repository Service).

SMKI SEC Documents has the meaning given to that expression in Section L9.4 (the SMKI SEC Documents).

SMKI Service Interface has the meaning given to that expression in Section L4.3 (the SMKI Service Interface).

SMKI Services has the meaning given to that expression in Section L3.1 (the SMKI Services).

SMKI Specialist means an individual (rather than a body corporate, association or partnership) to be appointed and remunerated under a contract with SECCo, who:
(a) has experience and expertise in public key infrastructure arrangements;
(b) is sufficiently independent of any particular Party or RDP, or class of Parties or RDPs, and of the Independent SMKI Assurance Service Provider; and
(c) is chosen by the SMKI PMA Chair from time to time.

SOC2 means the Service Organisation Control 2 standard, as defined by the American Institute of Certified Public Accountants.

SoLR Change of Supplier Processes

means, in relation to the Devices forming part of a Smart Metering System for a premises of a Pre-Payment Consumer of a Failing Energy Supplier, the replacement of any Device Security Credentials on those Devices that pertain to the Failing Energy Supplier with those that pertain to the Supplier of Last Resort.

Solution Architecture Information

means a description of the overall technical architecture of the DCC Systems (or any part thereof) in more detail than the Technical Architecture Document so as to describe the individual components of the DCC Systems (including hardware and software) and how they interface with the User Systems.

Special Installation Mesh Communications Hub

means a WAN Variant (in the central Region and the south Region) which is distinguishable from a standard Mesh Communications Hub by the existence of an additional external aerial port.

Special Second-Fuel Installation

means, in the case of a premises for which there is both an Electricity Smart Meter and a Gas Smart Meter, where on the installation of the second of those two meters to be installed it was necessary to replace the Communications Hub relating to the first of those two meters to be installed because that Communications Hub was not able to serve the second of those two meters to be installed (with the consequence that the Communications Hub that is replaced is removed from the premises and returned to the DCC).

Special WAN-Variant Installation

means that the DCC requests (in accordance with the Incident Management Policy) that a Supplier Party replaces an installed Communications Hub with a Communications Hub of a different WAN Variant to the installed Communications Hub, with the consequence that the Communications Hub that is replaced is removed from the premises and returned to the DCC.

Specimen Accession Agreement

means the specimen form of agreement set out in Schedule 2.

Specimen Bilateral Agreement

means the specimen form of agreement set out in Schedule 3.

Specimen Enabling Services Agreement

means the form of specimen agreement set out in Schedule 7 (Specimen Enabling Services Agreement).

SSC Guidance for Device Security Assurance and Triage means the document of that name developed by the SSC in accordance with Section G7.19(g).

SSI Baseline Requirements Document means a document produced and maintained by the DCC in accordance with the Self-Service Interface Access Control Specification.

SSI Change Governance Process means a document established under Section H8.15A (Self-Service Interface) and contains the governance arrangements for making changes to the Self-Service Interface.

Stage 1 Assurance Report has the meaning given to that expression in Part 4.4 of the SMKI Compliance Policy (Nature of the Initial Assessment).

Stage 2 Assurance Report has the meaning given to that expression in Part 4.6 of the SMKI Compliance Policy (Nature of the Initial Assessment).

Standalone Auxiliary Proportional Controller means a device installed (or to be installed) at a premises, which:
(a) consists of the components or other apparatus identified in; and
(b) as a minimum, has the functional capability specified by and complies with the other requirements of,
a Version of the SAPC Technical Specification which was within its Installation Validity Period on the date on which the device was installed.

Statement of Service Exemptions means a statement of that name developed by the DCC in accordance with Condition 17 of the DCC Licence.

Sub-Committee has the meaning given to that expression in Section C6 (Sub-Committees).

Sub GHz Alert Has the meaning given to 'Sub GHz Alert' in the GB Companion Specification.

Sub GHz Available Channels Has the meaning given to 'Sub GHz Available Channels' in the GB Companion Specification.

Subject in relation to a Certificate, has the meaning given to that expression in the relevant Certificate Policy.

Sub-Processor means, in respect of a Party which Processes Personal Data obtained pursuant to this Code as a Data Processor, any person which Processes such Personal Data on behalf of such Party.

Subscriber means, in relation to any Certificate, SECCo, a Party or an RDP which has been Issued with and accepted that Certificate, acting in its capacity as the holder of the Certificate.

Subscriber Obligations means the provisions in respect of Subscribers set out at Section L11 of the Code (the Subscriber Agreement Obligations).

Sub-Version in relation to:
(a) a Technical Specification, has the meaning given to that expression in Section A3.5(b) (Versions of the Technical Specifications); and
(b) the GBCS or CPA Security Characteristics, has the equivalent meaning, in accordance with and subject to the provisions of Section A3.27 (GB Companion Specification and CPA Security Characteristics).

Successfully Executed means:
(a) in respect of a Command and a Device, that the action that a Command of the relevant type is designed to effect in respect of a Device of the relevant Device Type has been effected on the Device;
(b) in respect of a Service Request and a Device, that the associated Command has been Successfully Executed on the Device as described in (a) above (or, in the case of Service Requests that are not designed to result in a Command, that the action that a Service Request of the relevant type is designed to effect has been effected); or
(c) in respect of a SMETS1 Service Request and a Device, that the Equivalent Steps have been successfully carried out.

Successor Licensee has the meaning given to that expression in Section M9.2 (Application and Interpretation of Section M9).

Supplementary Remote Party has the meaning given to that expression in the GB Companion Specification.

Supplier Certificates means, in respect of a Supplier Party, any Certificate or DCCKI Certificate for which the Supplier Party is a Subscriber or a DCCKI Subscriber.

Supplier of Last Resort

means, in respect of each premises supplied by a Failing Energy Supplier, the Supplier Party directed to supply gas and/or electricity to that premises by the Authority under a Last Resort Supply Direction (as defined in the Energy Supply Licences).

Supplier Party

means a Party that is an Electricity Supplier Party and/or a Gas Supplier Party.

Supply Meter Point

has the meaning given to that expression in the UNC.

Supply Meter Point Reference Number

has the meaning given to that expression in the UNC.

Supply of Energy

means either or both of the supply of gas pursuant to the Gas Act and the supply of electricity pursuant to the Electricity Act (in each case within the meaning that is given to the expression “supply” in the respective Act).

Supply Sensitive Check

means a check carried out by a User in relation to a Supply Sensitive Service Request in order to confirm the intention of the User that the associated Command(s) should be executed on the relevant Device, having regard to the reasonably foreseeable effect that the Command(s) could have on the quantity of gas or electricity that is supplied to a consumer at premises.

Supply Sensitive Service Request

means any Service Request in respect of which it is reasonably foreseeable that the associated Command(s), if it were to be executed on the relevant Device, could affect (either directly or indirectly) the quantity of gas or electricity that is supplied to a consumer at premises.

Suspended

means, in respect of a Device, that the Device has been suspended (or deemed suspended) in accordance with Section H6.10 (Suspension); and the word “**Suspension**” shall be interpreted accordingly.

Symmetric Key

means the Contingency Symmetric Key and any key derived from a Shared Secret in accordance with the GB Companion Specification.

System

means a system for generating, sending, receiving, storing (including for the purposes of Back-Up), manipulating or otherwise processing electronic communications, including all hardware, software, firmware and Data associated therewith.

System Development Lifecycle

means, in relation to any System, the whole of the life of that System from its initial concept to ultimate disposal, including the stages of development, design, build, testing, configuration, implementation, operation, maintenance, modification and decommissioning.

Tailored Assurance Service (CTAS)

means the scheme of that name which is administered by NCSC, or any successor to that scheme.

Target Availability Period

means, in relation to each DCC Interface (excluding the one listed in paragraph (f) of the definition of DCC Interface), a period of time in respect of each month, expressed in minutes and calculated as:
(a) the total number of minutes in that month, minus
(b) the number of minutes during which the DCC has, acting in compliance with Sections H8.2 and H8.3 (Maintenance of the DCC Systems), arranged for the given DCC Interface to be unavailable during that month for the purposes of Planned Maintenance.

Target Initial Response Time

means the time period within which an Incident within each Incident Category is to be recorded on the Incident Management Log and assigned to a resolver, as set out in the Incident Management Policy.

Target Resolution Time

has the meaning given to that expression in Section H9.1 (Incident Management Policy).

Target Response Time

has the meaning given to that expression in Section H3.14 (Target Response Times) or L8 (SMKI Performance Standards and Demand Management).

Target Service Level

means, in respect of each Performance Measure, the number or percentage intended to represent a reasonable level of performance for the activity which is the subject of the Performance Measure, as set out in:
(a) Section D11.1 (Code Performance Measures);
(b) Section H13.1 (Code Performance Measures);
(c) the Reported List of Service Provider Performance Measures; or
(d) Section L8.6 (Code Performance Measures).

TCH Participant

has the meaning given to that expression in Section F10.5 (Provision of Test Communications Hubs).

Technical Architecture and Business Architecture Sub-Committee means the Sub-Committee established pursuant to Section F1 (Technical Architecture and Business Architecture Sub-Committee).

Technical Architecture Document means a document setting out a representation of the End-to-End Technical Architecture.

Technical Code Specifications means the Technical Specifications, the GB Companion Specification, the DCC Gateway Connection Code of Connection, the DCC User Interface Code of Connection, the DCC User Interface Specification, the Self-Service Interface Access Control Specification, the Self-Service Interface Code of Connection, the Registration Data Interface Documents, the Message Mapping Catalogue, the Incident Management Policy, the DCC Release Management Policy, the SEC Release Management Policy, the SMKI Interface Design Specification, the SMKI Code of Connection, the SMKI Repository Interface Design Specification, the SMKI Repository Code of Connection, and the SMETS1 Supporting Requirements.

Technical Specification means each of the CHTS, the ESMETS, the GSMETS, the HCALCSTS, the IHDTS, the PPMIDTS and the SAPCTS.

Test Certificate means a certificate that simulates the function of a Certificate for the purpose of testing pursuant to this Code.

Test Communications Hub means:

(a) until such date as the DCC may determine (or such earlier date as the Secretary of State may designate for the purposes of this definition), a Prototype Communications Hub; and

(b) after such date, a device that is equivalent to a SMETS2+ Communications Hub but which contains such variations in functionality as the DCC reasonably considers appropriate to enable the device to be used for the purposes of testing, which device is provided (or to be provided) for the purpose of testing as described in Section F10 (Test Communications Hubs).

Test Repository means a repository that simulates the function of the SMKI Repository for the purpose of testing pursuant to this Code.

Test Stubs

means Systems and actions which simulate the behaviour of Devices and User Systems.

Testing Issue

means, in respect of any tests:
(a) anything that is preventing the execution of the tests; or
(b) once commenced or executed, the test has an unexpected or unexplained outcome or response.

Testing Participant

means, in respect of each Testing Service, the persons (whether or not they are Parties) who are entitled to undertake such tests, as described in Section H14 (Testing Services).

Testing Service

has the meaning given to that expression in Section H14.1 (General Testing Requirements).

Threshold Anomaly Detection

means the DCC processes which:

a. in respect of any User ID used by a User in one or more of its User Roles, detect whether the total number of communications (in general or of a particular type) sent, received or processed by the DCC in relation to that User ID exceeds the relevant Anomaly Detection Threshold;
b. in respect of the DCC (including when acting as a DCO, the CoS Party or a SMETS1 Service Provider), detect whether:
    i. the total number of communications of a particular type generated, sent, received or processed by the DCC in relation to all Users and the CoS Party exceeds the relevant Anomaly Detection Threshold; and
    ii. a data value within a communication of a particular type sent, received or processed by the DCC in relation to a User exceeds or is less than the relevant Anomaly Detection Threshold; and
c. (other than in the case of Threshold Anomaly Detection applied by a DCO) quarantine those communications that, in the case of paragraph (a) or (b)(i) above, are in excess of the relevant Anomaly Detection Threshold or, in the case of paragraph (b)(ii) above, contain a data value that exceeds or is less than the relevant Anomaly Detection Threshold.

Threshold Anomaly Detection Procedures

means the SEC Subsidiary Document of that name set out in Appendix AA, which has the purpose described in Section G6.1 (Threshold Anomaly Detection Procedures).

Transfer Date has the meaning given in Section F6A.4 (Communications Hub Transfer Requests), subject to change in accordance with the CH Handover Support Materials.

Transfer Location has the meaning given in Section F6A.4 (Communications Hub Transfer Requests).

Transform means, in respect of a Service Request in relation to a Device, the conversion of that Service Request into one or more corresponding Commands (less any required Message Authentication Code or Digital Signatures), where such correspondence is identified in the DCC User Interface Specification in respect of particular types of Service Request and particular Device Types; and "**Transformed**" shall be interpreted accordingly.

Transition and Migration Approach Document means the SEC Subsidiary Document set out in Appendix [TBC].

Transition Objective has the meaning given to that expression in Section X1 (General Provisions Regarding Transition).

Transport Layer Security means TLS in accordance with the relevant SMKI PMA and SSC Guidance (Standards, Procedures and Guidelines) published on the SEC website.

Trial Device Approval has the meaning given to that expression in Section F2.18 (Device Trials).

Trial Device Certificate has the meaning given to that expression in Section F2.25 (Device Trials).

Trial Device Model has the meaning given to that expression in Section F2.18 (Device Trials).

Trial Device Remedial Plan has the meaning given to that expression in Clause 6.3(b) of Appendix Z (CPL Requirements Document).

TS Applicability Tables means the document set out in Schedule 11 which has the content described at Section A3.32 (The TS Applicability Tables).

Type 1 Device means a HAN Connected Auxiliary Load Control Switch or a Pre-Payment Meter Interface Device.

Type 2 Device has the meaning given to that expression in the Technical Specification in which the expression is used (or given to the expression 'Consumer Device' in SMETS1).

Type 2 Device (Other) means a Type 2 Device that is not an IHD.

UKAS means the United Kingdom Accreditation Service

Unambiguous Consent means the explicit and informed consent of an Energy Consumer given to a User to undertake a specified action, and that consent shall not be treated as having been given explicitly unless the Energy Consumer has:

(a) of his or her own volition, communicated to the User a request for it to undertake that action; or

(b) in response to a specific request by the User for him or her to indicate consent to it undertaking that action, taken a positive step amounting to a clear communication of that consent.

UNC means the Uniform Network Code established pursuant to the Gas Transporter Licences.

Unique Transaction Reference Number (UTRN) has, where used in relation to a SMETS2+ Device, the meaning given to that expression in the GB Companion Specification; or, where used in relation to SMETS1 Device, has the meaning set out in SMETS1.

Unknown Remote Party for SMETS2+ Devices, has the meaning given to that expression in the GB Companion Specification; and, for SMETS1 Devices, has the meaning set out in the SMETS1 Supporting Requirements.

Unplanned Maintenance means, in respect of a month, Maintenance of the DCC Systems that was not planned prior to the start of that month and which disrupts, will disrupt, or poses a Material Risk of disruption to, provision of the Services (and, where it disrupts, will disrupt, or poses a Material Risk of disruption to, the provision of the Services in relation to Devices associated with Communications Hubs, at least 100,000 Communications Hubs are affected).

Unsecured Credit Factor Percentage has the meaning given to that expression in Section J3.10 (Party's Unsecured Credit Factor Percentage).

Unsecured Credit Limit has the meaning given to that expression in Section J3.7 (Party's Unsecured Credit Limit).

Upgrade Image shall have the meaning given to that expression in the SMETS1 Supporting Requirements.

UPRN means the unique property reference number (if any) recorded in respect of a premises so as to link the MPAN(s) and MPRN for that premises.

Urgent DCC Assessment means a DCC Assessment in respect of an Urgent Modification Proposal.

Urgent Proposal has the meaning given to that expression in Section D4.6 (Urgent Proposals).

User means a Party that has completed the User Entry Process (and, in respect of Services available in accordance with this Code to Users acting only in one or more User Roles, a Party that has completed the User Entry Process for that User Role).

User Entry Process means the process described in Section H1 (User Entry Process).

User Entry Process Tests means the tests described in Section H14.13 (User Entry Process Tests).

User ID means, in respect of a User and a User Role, one of the unique identification numbers accepted by the DCC in respect of that User and that User Role under Section H1.6 (User Roles and User IDs).

User Independent Security Assurance Service Provider has the meaning given to that expression in Section G8.1 (Procurement of the Independent Security Assurance Service Provider).

User Personnel means those persons who are engaged by a User, in so far as such persons carry out, or are authorised to carry out, any activity in relation to the business of the User in the exercise of rights and compliance with obligations under this Code.

User Privacy Self-Assessment

has the meaning given to that expression in Section I2.12 (Categories of Assessment).

User Privacy Self-Assessment Report

has the meaning given to that expression in Section I2.24 (The User Privacy Self-Assessment Report).

User Role

means, in respect of the Service set out in the DCC User Interface Services Schedule and Elective Communication Services, one of the categories of User that is capable of being an Eligible User in respect of those Services (determined without reference to a particular Smart Metering System), and which comprise the following categories (construed without reference to a particular Smart Metering System): Import Supplier, Export Supplier, Gas Supplier, Electricity Distributor, Gas Transporter, Registered Supplier Agent and Other User.

User Security Assessment

means either a Full User Security Assessment or a Verification User Security Assessment.

User Security Assessment Methodology

means a methodology to be applied (as the case may be):
(a) by the User Independent Security Assurance Service Provider in carrying out any User Security Assessment; or
(b) by a User, in carrying out any User Security Self-Assessment,
in each case in accordance with the provisions of the Security Controls Framework applicable to the relevant category of security assurance assessment.

User Security Assessment Report

has the meaning given to that expression in Section G8.22 (User Security Assessments: General Procedure).

User Security Assessment Response

has the meaning given to that expression in Section G8.24 (User Security Assessments: General Procedure).

User Security Self-Assessment

has the meaning given to that expression in Section G8.18 (Categories of Security Assurance Assessment).

User Systems

means any Systems (excluding any Devices) which are operated by or on behalf of a User and used in whole or in part for:
(a) constructing Service Requests;
(b) sending Service Requests over the DCC User Interface;
(c) receiving, sending, storing, using or otherwise carrying out any processing in respect of any Pre-Command or Signed Pre-Command;
(d) receiving Service Responses or Alerts over the DCC User Interface;
(e) generating Data for communication to the OCA, DCA, ICA or DCCKICA, or receiving Data from the OCA, DCA, ICA or DCCKICA (including any Systems which store or use Secret Key Material for such purposes) but excluding communications in relation to Devices that do not have an SMI Status of "commissioned" or "installed not commissioned"; and/or
(f) generating any Unique Transaction Reference Number,
and any other Systems from which the Systems used in whole or in part for the purposes set out in paragraphs (a) to (f) are not Separated.

UTC (Coordinated Universal Time)

means the prime standard by which clocks and time are regulated.

Valid Communications Hub Order

means the Consignment or Consignments which arise from a Communications Hub Order that has been accepted by the DCC under Section F5.16 or F5.17 (DCC: Duties in relation to Communications Hub Orders), and which have not been cancelled by the ordering Party in accordance with Section F5.19 (Non-Standard Cancellation of Consignments).

Validity Period

has the meaning given to that expression in any of the Certificate Policies or the DCCKI Certificate Policy.

Value at Risk

has the meaning given to that expression in Section J3.6 (Party’s Value at Risk).

VAT

means VAT, as defined in the Value Added Tax Act 1994, and any tax of a similar nature which may be substituted for or levied in addition to it.

Verification User Security Assessment

has the meaning given to that expression in Section G8.17 (Categories of Security Assurance Assessment).

Verify

means, in respect of a Service Request or Signed Pre-Command, to confirm that it meets all the applicable requirements of the DCC User Interface Specification.

Version

in relation to:

a. a Technical Specification, has the meaning given to that expression in Section A3.2 (Versions of the Technical Specifications);

b. the GBCS or CPA Security Characteristics, has the meaning given to that expression in Section A3.26 (GB Companion Specification and CPA Security Characteristics); and

c. the DCC User Interface Specification, has the meaning given to that expression in Section A3.36 (DCC User Interface Specification and Message Mapping Catalogue),

and in the case of Technical Specifications, the GBCS or CPA Security Characteristics includes both the Principal Version and Sub-Version of that document. The concepts of Principal Version and Sub-Version do not apply to the DCC User Interface Specification.

Volume Scenarios

means the capacity levels to which the DCC Systems will be tested.

Voting Group

means, in respect of each Party Category, each Party that falls into that Party Category collectively with that Party's Affiliates (if any) who also fall into that Party Category.

WAN Variants

means the variations of SMETS2+ Communications Hub that are necessary to enable communications via the SMETS2+ SM WAN in each Region (and each part thereof that is not subject to the Statement of Service Exemptions).

Website

means a dedicated website established at the direction of the Panel for the purposes of this Code.

Wide Area Network (WAN) Provider

means the DCC, acting in the capacity and exercising the functions of the Known Remote Party role identified as such in the GB Companion Specification.

Wired Instrumented Test Communications Hubs (Wired ITCH)

means the Testing Service described in Section H14.54 (Wired Instrumented Test Communications Hubs).

Working Day

means any day other than a Saturday, a Sunday, Christmas Day, Good Friday, or a day that is a bank holiday within the meaning of the Banking and Financial Dealings Act 1971.

Working Group has the meaning given to that expression in Section D6.2 (Establishment of a Working Group).

Working Group Terms of Reference has the meaning given to that term in Section D6.2 (Establishment of a Working Group).

XML User Role Signing Private Key means a Private Key associated with a Public Key that is contained within an Organisation Certificate with a Remote Party Role of "xmlSign".

Zigbee Alliance means the association of that name administered by ZigBee Alliance Inc (2400 Camino Ramon, Suite 375, San Ramon, CA 94583, USA) (see - www.zigbee.org).

A2. INTERPRETATION

A2.1 In this Code, unless the context otherwise requires, any reference to:

(a) a “person” includes a reference to an individual, a body corporate, an association, a partnership or a Competent Authority;

(b) the singular includes the plural, and vice versa;

(c) a gender includes every gender;

(d) a Section or Schedule is a reference (respectively) to the section of, or schedule to, this Code which bears the relevant letter, number or letter and number;

(e) a numbered Paragraph or a numbered Clause is a reference to the paragraph or clause of the Schedule or Appendix in which such reference occurs;

(f) a numbered Condition (with or without a letter) is a reference to the licence condition bearing that number (and, where relevant, letter) in the Energy Licence indicated (and, save in the case of the DCC Licence, is a reference to the standard licence conditions of that Energy Licence);

(g) writing (or similar) includes all methods of reproducing words in a legible and non-transitory form (including email);

(h) a day, week or month is a reference (respectively) to a calendar day, a week starting on a Monday, or a calendar month;

(i) a time is a reference to that time in the UK;

(j) any statute or statutory provision includes any subordinate legislation made under it, any provision which it has modified or re-enacted, and any provision which subsequently supersedes or re-enacts it (with or without modification);

(k) an agreement, code, licence or other document is to such agreement, code, licence or other document as amended, supplemented, novated or replaced from time to time;

(l) a Party shall include reference to that Party's respective successors, (in the case of the DCC) to the person to whom the DCC may novate its rights and obligations pursuant to Section M9 (Transfer of DCC Licence), and (as the context permits) reference to the respective persons to whom that Party may sub-contract or otherwise delegate its rights and/or obligations under this Code in accordance with Section M11.8 and M11.9 (which shall include, in the case of the DCC, reference to the DCC Service Providers);

(m) any premises of a Party shall include references to any premises owned or occupied by that Party and (as the context permits) by the respective persons to whom that Party may sub-contract or otherwise delegate its rights and/or obligations under this Code in accordance with Section M11.8 and M11.9 (which shall include, in the case of the DCC, reference to the DCC Service Providers);

(n) a Competent Authority or other public organisation includes a reference to its successors, or to any organisation to which some or all of its functions and responsibilities have been transferred; and

(o) an expression that is stated to have the meaning given to it in an Energy Licence (other than the DCC Licence) is a reference to that expression as defined in the standard licence conditions for the Energy Licence indicated.

A2.2 The headings in this Code are for ease of reference only and shall not affect its interpretation.

A2.3 In this Code, the words preceding "include", "including" or "in particular" are to be construed without limitation to the generality of the words following those expressions.

A2.4 The language of this Code is English. All notices and other communications sent between any of the Parties, the Panel, SECCo, the Code Administrator and the Secretariat shall be in English.

A2.5 Except where expressly stated to the contrary, in the event of any conflict between the provisions of this Code, the following order of precedence shall apply:

(a) the Sections, as among which Section X (Transition) shall take precedence; then

(b) the Schedules; then

(c) the SEC Subsidiary Documents.

A2.6 Section A2.7 shall apply, during the period prior to Completion of Implementation, where initial capital letters are used for any expression in this Code that either is not defined in this Code or the definition of which cannot be given effect by reference to the provisions of this Code.

A2.7 Any expression of the type referred to in Section A2.6 shall be interpreted as having the meaning given to that expression in the decision or consultation document concerning the intended future definition of such expression most recently published by the Secretary of State prior to the date on which this Section A2.7 comes into force.

A2.8 Where no time period is specified for performance of any obligation under this Code, the obligation shall be performed as soon as reasonably practicable.

A2.9 Where any expression is defined both in Section A1 (Definitions) and in any Schedule or Appendix:

(a) the definition in the Schedule or Appendix shall take precedence for the purposes of that Schedule or Appendix (including for the purposes of any Technical Specification included within any such Schedule); and

(b) the definition in Section A1 shall take precedence for all other purposes

A2.10 For the purposes of Section A2.9, where the meaning of an expression is explained in any glossary (or equivalent section) of a Schedule which includes a Technical Specification, it shall be treated as an expression that is defined in each Technical Specification that is included within that Schedule.

A2.11 Where any Data is:

(a) embedded as a file within the electronic copy of any Technical Specification, the GBCS, the DCC User Interface Services Schedule or the Message Mapping Catalogue; and/or

(b) represented within the tangible copy of that document as being so embedded,

A2.12 In this Code, each reference to the term or expression:

(a) 'Smart Metering Equipment Technical Specifications';

(b) 'SMETS',

shall be read, as the context requires, as a reference to the ESMETS, the GSMETS, the IHDTS, the HCALCSTS, the PPMIDTS, or the SAPCTS (or to any two or more (or all) of them).

A3. TECHNICAL SPECIFICATIONS, THE GB COMPANION SPECIFICATION, THE CPA SECURITY CHARACTERISTICS, AND THE DCC USER INTERFACE SPECIFICATION

Introduction

A3.1 This Section A3 makes provision in relation to:

(a) the maintenance in this Code of different versions of each of the Technical Specifications;

(b) the relationship between each version of a Technical Specification and:

(i) the GB Companion Specification; and

(ii) the CPA Security Characteristics; and

(c) the interpretation of the Code in respect of the Technical Specifications, GB Companion Specification, CPA Security Characteristics, the DCC User Interface Specification, and the Message Mapping Catalogue.

Versions of the Technical Specifications

A3.2 Each Technical Specification may exist in more than one version (a "**Version**").

A3.3 Each Version of a Technical Specification shall consist of two elements:

(a) a Principal Version; and

(b) a Sub-Version of that Principal Version.

A3.4 Each Version of a Technical Specification shall be identified by a numerical reference in a form equivalent to 'ESMETS v 1.2', where:

(a) the number before the decimal point identifies the Principal Version; and

(b) the number after the decimal point identifies the Sub-Version.

A3.5 In respect of any Technical Specification:

(a) the expression "**Principal Version**" shall be interpreted in accordance with Sections A3.6 to A3.7; and

(b) the expression "**Sub-Version**" shall be interpreted in accordance with Sections A3.8 to A3.9.

The Principal Version

A3.6 Where a Technical Specification is amended in a manner that is entirely prospective, that amendment shall be made by creating a new Principal Version, and:

(a) for this purpose a prospective amendment means one that does not require any change to be made to any Device or apparatus which is already installed;

(b) in consequence a new Principal Version shall be taken to indicate amendments which have no retrospective effect.

A3.7 The first Principal Version of:

(a) each of the ESMETS, the GSMETS, the IHDTS and the CHTS shall be allocated the number 1, and subsequent Principal Versions of each such that Technical Specification shall be allocated sequential numbers;

(b) (b) each of the PPMIDTS, the HCALCSTS and the SAPCTS shall be allocated the number 2, and subsequent Principal Versions of each such Technical Specification shall be allocated sequential numbers.

The Sub-Version

A3.8 Where any Principal Version of a Technical Specification is amended in a manner that is intended to have retrospective effect, that amendment shall be made by creating a new Sub-Version, and for these purposes:

(a) a Sub-Version means a new form of the Principal Version to which it relates;

(b) an amendment with retrospective effect means one that requires a change to be made to Devices or apparatus which are already installed.

A3.9 The initial form of a Principal Version of a Technical Specification shall be allocated the Sub-Version number of zero, and subsequent Sub-Versions shall be allocated sequential numbers, beginning with 1, in the chronological order in which they are created.

The Installation Validity Period

A3.10 Any Version of a Technical Specification may be assigned an Installation Validity Period.

A3.11 An "**Installation Validity Period**" means the period of time during which any Device or apparatus satisfying the requirements of that Version of the Technical Specification may be installed or provided.

A3.12 An Installation Validity Period shall:

(a) commence on the "**Installation Start Date**" that is identified in relation to that Version of the Technical Specification in the TS Applicability Tables; and

(b) end on any "**Installation End Date**" determined in accordance with Sections A3.13 to A3.16.

The Installation End Date

A3.13 In the case of each Version of the ESMETS, the GSMETS and the IHDTS with a Principal Version number of 1, the Installation End Date shall, except where Section A3.14 or Section A3.15 applies, be the date which is identified in relation to that Version in the TS Applicability Tables as the "**General Installation End Date**".

A3.14 This section applies on the installation or provision by or on behalf of a Supplier Party of any Replacement Meter and ancillary Device or apparatus where:

(a) the Energy Meter that is being replaced is not part of a Smart Metering System; and

(b) the Replacement Meter is, in accordance with the terms of a contract between the Supplier Party and the Energy Consumer at the premises at which it is installed, to be operated as a Pre-Payment Meter for at least an initial period from the date of its installation,

in which case the Installation End Date in respect of any Version of the ESMETS, the GSMETS and the IHDTS with a Principal Version number of 1 shall be the date which is identified in relation to that Version in the TS Applicability Tables as the "**PPM Installation End Date**".

A3.15 This Section applies where a Derogation is granted to a Supplier Party in accordance with Section A4 (Derogation from General Installation End Date) and has not been revoked, in which case:

(a) for the purposes of the installation or provision by or on behalf of that Supplier Party of any Device or apparatus; and

(b) in so far as any conditions of that Derogation are satisfied,

the Installation End Date shall be the Alternative Installation End Date specified in the Derogation.

A3.16 In the case of each Version of a Technical Specification, other than the ESMETS, the GSMETS and the IHDTS with a Principal Version number of 1, the Installation End Date shall be the date that may be identified in relation to that Version of the Technical Specification in the TS Applicability Tables.

A3.17 The Installation End Date of any Version of a Technical Specification may be later than the Installation Start Date of a Version that succeeds it, so that:

(a) two or more Versions may be within their Installation Validity Periods at the same time; and

(b) any Device or apparatus to which each such Version relates may be installed or provided in accordance with any such Version that is within its Installation Validity Period at that time.

The Maintenance Validity Period

A3.18 Each Version of a Technical Specification shall be assigned a Maintenance Validity Period.

A3.19 A "**Maintenance Validity Period**" means:

(a) the period of time during which a Device or other apparatus may be maintained in accordance with the requirements of that Version of the Technical Specification; and

(b) the period of time during which User can interface to the DCC in accordance with that Version of the DCC User Interface Specification.

A3.20 A Maintenance Validity Period shall:

(a) commence on the "**Maintenance Start Date**" that is identified in relation to that Version of the Technical Specification or the DCC User Interface Specification in the TS Applicability Tables; and

(b) end on any "**Maintenance End Date**" that may be identified in relation to that Version of the Technical Specification or the DCC User Interface Specification in the TS Applicability Tables.

A3.21 The Maintenance End Date of any Version of a Technical Specification may be later than the Maintenance Start Date of a Version that succeeds it, so that:

(a) two or more Versions may be within their Maintenance Validity Periods at the same time; and

(b) any Device or apparatus to which each such Version relates may be maintained in accordance with any such Version that is within its Maintenance Validity Period at that time.

Versions in the Code

A3.22 Each Version of a Technical Specification or DCC User Interface Specification shall be retained in the relevant Schedule to the Code at all times during which it remains within its Installation Validity Period (if any) and/or its Maintenance Validity Period.

A3.23 Where, in respect of any Version of a Technical Specification or DCC User Interface Specification:

(a) no Installation Validity Period has been assigned, or any Installation Validity Period that was assigned has expired; and

(b) the Maintenance Validity Period has expired, that Version shall be deemed automatically to be deleted from the Code on the day immediately following whichever is the later of its Installation End Date (if any) or Maintenance End Date, and the part of the Schedule or the part of the composite document in the Schedule (as the case may be) in which it is set out shall then automatically be marked 'Not Used'.

A3.24 The Code Administrator shall at all times maintain on the Website copies of those Versions of each Technical Specification, DCC User Interface Specification and Message Mapping Catalogue which have been deleted from the Code in accordance with Section A3.23, together with a record of the Installation Start and End Dates (if any) and the Maintenance Start and End Dates relating to each such Version.

GB Companion Specification and CPA Security Characteristics

A3.25 The GB Companion Specification and the CPA Security Characteristics may each exist in more than one version (a "**Version**").

A3.26 The provisions of Sections A3.3 to A3.9 shall apply to the GBCS and CPA Security Characteristics:

(a) as if references in those Sections to a Technical Specification were references to each of those documents; and

(b) in respect of the CPA Security Characteristics, so that:

(i) any reference in those Sections to the creation of a new Version by an amendment that requires a change to be made to a Device or apparatus which is already installed shall be read as if it were a reference to an amendment requiring the Device Model of a Device or apparatus which is already installed to be certified, on the expiry of its CPA Certificate, against the new Version of the CPA Security Characteristics; and

(ii) Section A3.38 shall be interpreted accordingly.

A3.27 The provisions of Sections A3.22 to A3.24 shall apply to the GBCS as if references in those Sections:

(a) to a Technical Specification were references to the GBCS;

(b) to an Installation Validity Period or Maintenance Validity Period were to an Applicability Period; and

(c) to an Installation Start or End Date, or a Maintenance Start or End Date, were to the first and last dates of the Applicability Period.

A3.28 Each Technical Specification requires that the Device or other apparatus to which it relates must be compatible with a relevant Version of the GBCS.

A3.29 For these purposes:

(a) the relevant Version of the GBCS in relation to any Version of a Technical Specification shall be deemed to be that which is specified in relation to it in the TS Applicability Tables;

(b) more than one Version of the GBCS may be relevant to a Version of a Technical Specification at the same time;

(c) a Version of the GBCS may be relevant to more than one Version of a Technical Specification at the same time;

(d) a Version of the GBCS shall be relevant to a Version of a Technical Specification only during such period of time (in each case, an "**Applicability Period**") as may be specified in the TS Applicability Tables.

A3.30 Each Version of the GBCS requires that the Device or other apparatus must be certified as compliant with a relevant Version of the CPA Security Characteristics.

A3.31 For these purposes:

(a) the relevant Version of the CPA Security Characteristics in relation to any Version of the GBCS shall be deemed to be that which is specified in relation to it in the TS Applicability Tables;

(b) more than one Version of the CPA Security Characteristics may be relevant to a Version of the GBCS at the same time;

(c) a Version of the CPA Security Characteristics may be relevant to more than one Version of the GBCS at the same time.

The TS Applicability Tables

A3.32 There shall be a document to be known as the "**TS Applicability Tables**", which shall be set out at Schedule 11 to the Code following its initial designation in accordance with Section X5 (Incorporation of Certain Documents into this Code) by the Secretary of State in reliance on Section X5.4 (Other Technical Specifications), and shall:

(a) in relation to each Technical Specification, list each of the Versions of that Technical Specification that have been produced;

(b) in relation to each such Version of that Technical Specification, identify:

(i) any Installation Start Date that has been assigned to it;

(ii) in the case of each Version of the ESMETS, the GSMETS and the IHDTS with a Principal Version number of 1, the General Installation End Date that has been assigned to it;

(iii) in the case of each Version of a Technical Specification other than one identified in paragraph (ii), any Installation End Date that has been assigned to it (or a statement that no such date has yet been determined);

(iv) the Maintenance Start Date;

(v) the Maintenance End Date (or a statement that no such date has yet been determined);

(vi) the relevant Version(s) of the GBCS;

(vii) any Applicability Period relating to any such relevant Version of the GBCS;

(c) in relation to each Version of the GBCS, identify the relevant Version(s) of the CPA Security Characteristics;

(d) set out which version of each Technical Specification is contained within each of the documents contained within Schedule 9 of the Code; and

(e) In relation to each Version of the DUIS, identify:

(i) the date from which that Version becomes applicable; and

(ii) the date after which that Version ceases to be applicable (or a statement that no such date has yet been determined).

A3.33 The TS Applicability Tables shall be amended to ensure that it remains accurate and up-to-date:

(a) on the designation or re-designation of a Technical Specification or the GBCS in accordance with Section X5 (Incorporation of Certain Documents into this Code), by the Secretary of State in reliance on Section X5.6 (Supplementary Provisions); and

(b) as part of any modification of the Code which creates a new Version of any Technical Specification or of the GBCS in accordance with Section D (Modification Process).

A3.34 Where the TS Applicability Tables is amended (including by the means described in Section A3.33) the amendment may have retrospective effect, which is to say that any date specified in the TS Applicability Tables by virtue of that amendment may be a date which falls before the date on which the amendment was made.

A3.35 The information set out in the TS Applicability Tables shall be regarded as conclusive for all purposes of any question as to the:

(a) Installation Validity Period of any Version of a Technical Specification other than in any case where both:

(i) it is a Version of the ESMETS, the GSMETS and the IHDTS with a Principal Version number of 1; and

(ii) a Derogation has been granted to any Supplier Party in accordance with Section A4 (Derogation from General Installation End Date), and has not been revoked, specifying an Alternative Installation End Date in respect of that Version of the ESMETS, the GSMETS and the IHDTS;

(b) Maintenance Validity Period of any Version of a Technical Specification;

(c) relevant Version(s) of the GBCS in relation to any Version of a Technical Specification;

(d) Applicability Period of any Version of the GBCS;

(e) relevant Version(s) of the CPA Security Characteristics in relation to any version of the GBCS; and

(f) relevant Version or Versions of the DUIS which can be used at a given time by the DCC and Users.

DCC User Interface Specification and Message Mapping Catalogue

A3.36 The DCC User Interface Specification may exist in more than one version (a "**Version**"). Each such Version shall be subject to a "**Maintenance Validity Period**" which:

(a) commences on the start date that is identified in relation to that Version of the DCC User Interface Specification in the TS Applicability Tables; and

(b) ends on the Maintenance End date (if any) that may be identified in relation to that Version of the DCC User Interface Specification in the TS Applicability Tables.

A3.37 Where there is more than one Version of the DCC User Interface Specification:

(a) each such Version shall contain a different Version of the DUIS XML Schema (but a Version of the DCC User Interface Specification may be modified, and its version number updated, without any corresponding change to the DUIS XML Schema);

(b) there shall be, in respect of each such Version, one or more corresponding versions of the Message Mapping Catalogue;

(c) a User may submit any Service Request, in respect of which it is an Eligible User, in accordance with any Version of the DCC User Interface Specification which is (at the relevant time) within its Maintenance Validity Period;

(d) in accordance with the requirements of each version of the DCC User Interface Specification, each such Service Request must identify the Version of the DUIS XML Schema in accordance with which it has been submitted;

(e) any obligation on the DCC or any User in relation to any Service Request or associated communication shall be interpreted by reference to the provisions of the Version of the DCC User Interface Specification that contains the DUIS XML Schema that is identified in that Service Request;

(f) the obligation on the DCC at Section H11.1 (Parse and Correlate Software) to provide Parse and Correlate Software shall be interpreted as an obligation to provide a separate version of the Parse and Correlate Software in respect of each version of the DCC User Interface Specification (and each corresponding version of the Message Mapping Catalogue); and

(g) any other obligation on the DCC under this Code in relation to the Parse and Correlate Software shall be read as an obligation applying separately in respect of each such version of that software.

A3.37A Each Version of the DCC User Interface Specification shall be retained in the relevant Schedule to the Code at all times during which it remains within its Maintenance Validity Period. Where the Maintenance Validity Period of a Version of the DCC User Interface Specification has expired, then that Version (and any version of the Message Mapping Catalogue that corresponds only to that Version of DUIS as indicated by the Parse and Correlate Applicability Matrix) shall be deemed automatically to be deleted from the Code on the day immediately following the end of that DCC User Interface Specification's Maintenance Validity Period, and the part of the Schedules in which they are set out shall then automatically be marked 'Not Used'. The Code Administrator shall at all times maintain on the Website copies of those Versions of the DCC User Interface Specification and Message Mapping Catalogue which have been deleted from the Code in accordance with this Section A3.37A, together with a record of the Maintenance Validity Period relating to each such DCC User Interface Specification Version.

The Parse and Correlate Applicability Matrix

A3.38 There shall be a document to be known as the "**Parse and Correlate Applicability Matrix**", which shall include:

(a) a list of each of the versions of the Parse and Correlate Software that have been released; and

(b) in relation to each such version of the Parse and Correlate Software:

(i) its version number;

(ii) the version(s) of the DCC User Interface Specification to which that version of the Parse and Correlate Software relates, and the version of the DUIS XML Schema which that version of the DCC User Interface Specification contains;

(iii) the version(s) of the Message Mapping Catalogue to which that version of the Parse and Correlate Software relates;

(iv) the version(s) of the GBCS to which that version of the Parse and Correlate Software relates.

A3.39 The Code Administrator shall:

(a) maintain the Parse and Correlate Applicability Matrix to ensure that it remains accurate and up-to-date;

(b) ensure that the latest version of the Parse and Correlate Applicability Matrix is published and available on the Website.

A3.40 The DCC shall ensure that the Code Administrator is provided with such information as it requires for the purpose of complying with Section A3.39.

Interpretation

A3.41 References in this Section A3 to amendments of a Technical Specification which do (or do not) require changes to be made to any Device or apparatus which is already installed shall be interpreted as references to the effect of those amendments on the duties of:

(a) Electricity and Gas Supplier Parties in accordance with the standard conditions of the Energy Supply Licences; and

(b) the DCC in accordance with the conditions of the DCC Licence.

A3.42 Where:

(a) any provision of this Code relates to a Device or any communication to or from a Device; and

(b) the application of that provision requires that reference is made to a Version of a Technical Specification,

the Version of that Technical Specification which shall be treated as applicable for that purpose shall be the one identified as pertaining to the Device Model of that Device in the Central Products List.

A3.43 The references in this Code to 'Technical Specifications' shall be deemed not to include reference to Versions of the ESMETS, the GSMETS and the IHDTS with a Principal Version number of 1, except in the following provisions:

(a) the definitions of 'Principal Version', 'Sub-Version' and 'Version' in Section A1 (Definitions);

(b) Sections A2 (Interpretation), A3 (Technical Specifications, the GB Companion Specification and the CPA Security Characteristics); and A4 (Derogation from SMETS1 Generation Installation End Date); and

(c) Section N (SMETS1 Meters).

A4. DEROGATION FROM GENERAL INSTALLATION END DATE

Introduction

A4.1 This Section A4 makes provision for the Secretary of State to grant to any Supplier Party, on the application of that Party, a derogation from the General Installation End Date applicable to any Version of the ESMETS, the GSMETS and the IHDTS with a Principal Version number of 1.

Part A. Derogations

A4.2 For the purposes of this Section A4, a "Derogation" means a direction issued by the Secretary of State:

(a) to the Supplier Party which applied for it;

(b) in respect of a Version of the ESMETS, the GSMETS and the IHDTS with a Principal Version number of 1;

(c) specifying a date subsequent to the General Installation End Date in respect of that Version of the ESMETS, the GSMETS and the IHDTS (the "**Alternative Installation End Date**"), which will constitute the Installation End Date, in those cases which the PPM Installation End Date does not apply, for the purposes of the installation or provision of Devices or apparatus by or on behalf of the Supplier Party in accordance with any conditions of the Derogation;

(d) specifying any such conditions to which the Derogation is subject.

Part B. Power to Grant a Derogation

A4.3 The Secretary of State may grant a Derogation to any Supplier Party where:

(a) that Supplier Party has applied for a Derogation in accordance with Part D;

(b) that application complies with any requirements as to form or content set out in a statement issued in accordance with Part E;

(c) in the opinion of the Secretary of State, that application satisfies any criteria set out in a statement issued in accordance with Part E; and

(d) the Supplier Party has complied with all such other requirements as may apply to it in accordance with Part E.

Part C. Conditions of a Derogation

A4.4 A Derogation may be subject to such conditions (if any) as the Secretary of State thinks reasonable in all the circumstances of the case.

A4.5 The conditions to which a Derogation is subject may in particular include conditions which, in respect of the period that begins immediately after the General Installation End Date and ends on the Alternative

Installation End Date of the Version of the ESMETS, the GSMETS and the IHDTS to which the Derogation relates:

(a) place a limit on the quantity of Devices or apparatus which may be installed or provided by or on behalf of the Supplier Party to which the Derogation is granted;

(b) restrict the type of Devices or apparatus that may be installed or provided by or on behalf of that Supplier Party;

(c) make provision as to the circumstances in, or premises at, which such Devices or apparatus may be installed or provided by or on behalf of that Supplier Party;

(d) place requirements on that Supplier Party to take, or refrain from taking, any specified action in relation to the installation or provision of any Devices or apparatus.

Part D. Applications for a Derogation

A4.6 Any Supplier Party may apply to the Secretary of State for a Derogation.

A4.7 The Secretary of State may determine, and in that case shall give all Supplier Parties a notice of, a date by which any application for a Derogation must be received by him.

A4.8 A Supplier Party may not apply for a Derogation after any date that is determined and included in a notice given in accordance with Section A4.7.

Part E. Statement of Requirements

A4.9 The Secretary of State may determine, and publish a statement of:

(a) the criteria against which any application for a Derogation is to be assessed by him;

(b) any requirements as to the form and content of any such application;

(c) any information or evidence which must be provided by a Supplier Party on making such an application;

(d) any timetable which applies to steps to be taken by the Supplier Party or by the Secretary of State in respect of such an application;

(e) such other matters which relate to the making of any such application or to the process for assessing it as the Secretary of State may consider appropriate;

(f) such matters which relate to the decision whether to grant a Derogation on the receipt of an application, or to the conditions to be applied to that Derogation, as the Secretary of State may consider appropriate.

A4.10 A Supplier Party which applies for a Derogation shall:

(a) comply with any requirements applicable to it which are set out in a statement published in accordance with Section A4.9; and

(b) provide to the Secretary of State, by such time and in such form as he may reasonably specify in a notice given to that Supplier Party, such additional information or evidence as he may at any time reasonably require for the purpose of assessing the application.

Part F. Actions before this Section Comes into Force

A4.11 Where, prior to the coming into effect of this Section A4:

(a) a Supplier Party makes any application:

(i) that it would be entitled to make under this Section A4 after it has come into force; and

(ii) in respect of that application, has complied with the requirements of this Section A4 as if they had already come into force;

(b) the secretary of state takes any action that he would be entitled to take under this section A4 after it has come into force,

each of those sections shall be treated as actions taken and having effect under this Section A4 after it comes into force.

Part G. Amendments after this Section Comes into Force

A4.12 Where the Secretary of State has determined, and given all Supplier Parties notice of, a date in accordance with Section A4.7, he may subsequently (whether before or after that date has passed) determine and give all Supplier Parties notice of a later date.

A4.13 Any date determined and included in a notice given in accordance with Section A4.12 shall have effect for the purposes of Section A4.7 in replacement for the date that was previously determined by the Secretary of State.

A4.14 The Secretary of State may at any time:

(a) amend any statement published in accordance with Section A4.9, in which case the amended statement shall have effect for the purposes of Section A4.10 in replacement for the one that was previously published;

(b) in respect of the Derogation granted to any Supplier Party, vary:

(i) the Alternative Installation End Date, by specifying a date later than that previously specified;

(ii) any conditions to which the Derogation is subject, by imposing new or amended conditions.

A4.15 The Secretary of State may exercise the powers set out at Sections A4.12 and A4.14 on more than one occasion.

Part H. Revocation of Derogations

A4.16 The Secretary of State may at any time, by notice to the Supplier Party to which it was granted, revoke any Derogation granted by him in accordance with this Section A4.

Part I. Effect of a Derogation

A4.17 Where a Derogation is granted to a Supplier Party in accordance with this Section A4 and has not been revoked, then:

(a) for the purposes of the installation or provision by or on behalf of that Supplier Party of any Device or apparatus; and

(b) in so far as any conditions of that Derogation are satisfied, the Alternative Installation End Date specified in the Derogation shall have effect in accordance with Section A3.15 (The Installation End Date).

Part J. Publication of Derogations

A4.18 Where the Code Administrator is provided by the Secretary of State with a copy of a Derogation that has been granted by him to a Supplier Party, it shall:

(a) maintain a copy of that Derogation on the Website;

(b) if it is notified by the Secretary of State that the Derogation has been amended and provided by him with a copy of the amended Derogation, publish and maintain a copy of that amended Derogation on the Website;

(c) if it is notified by the Secretary of State that the Derogation has been revoked, publish on the Website, together with that Derogation, a statement of the fact that it has been revoked and the date of its revocation.

A4.19 For the purposes of Section A4.18, any reference to a copy of a Derogation provided to the Code Administrator by the Secretary of State shall, where that copy has been redacted by the Secretary of State to exclude any commercially sensitive information, be treated as a reference to the copy of that Derogation in its redacted form.

B ACCESSION

B1. ACCESSION

Eligibility for Admission

B1.1 Any person who applies to be admitted as a Party (an **Applicant**) shall be entitled to be admitted as a Party, subject to and in accordance with the provisions of this Section B1.

B1.2 An Applicant may not be admitted as a Party if:

(a) it is already a Party; or

(b) it was expelled from this Code in accordance with Section M8 (Suspension, Expulsion and Withdrawal) within the 12 months preceding the date of its application (or such shorter period as the Panel may determine from time to time).

Application Form and Guidance

B1.3 The Code Administrator shall create an Application Form, and publish such form on the Website.

B1.4 The Code Administrator shall establish and publish on the Website a guide for Applicants describing, and providing guidance in respect of, the process set out in this Section B1 (the **Application Guidance**).

Application Fee

B1.5 The Panel shall determine (and publish on the Website) a fee from time to time (the **Application Fee**) to be payable by Applicants to SECCo. The Panel shall set the Application Fee at a level intended to recover the reasonable costs incurred by or on behalf of the Panel (including amounts payable to the Code Administrator) in administering the process set out in this Section B1.

B1.6 The Code Administrator shall include within the Application Guidance details of the methods by which the Application Fee may be paid.

Accession Process

B1.7 An Applicant shall submit to the Code Administrator a duly completed Application Form (together with any supporting documents required by that form), and the Application Fee (by a method of payment provided for in the Application Guidance).

B1.8 As soon as reasonably practicable following receipt of an Application Form and the Application Fee from an Applicant, the Code Administrator shall:

(a) notify the Applicant if it is ineligible to be admitted as a Party in accordance with Section B1.2;

(b) where the Applicant is not ineligible, check that the Application Form has been duly completed and that any supporting documentation requested has been provided, and notify the Applicant of any omissions; and

(c) where there are no such omissions, notify the Applicant and the Panel that the Applicant is to be admitted as a Party subject to execution of an Accession Agreement.

Accession Agreement

B1.9 Where an Applicant is to be admitted as a Party in accordance with Section B1.8(c), the Code Administrator shall prepare two counterparts of the Accession Agreement for the Applicant (in substantially the form of the Specimen Accession Agreement), and send them to the Applicant.

B1.10 An Applicant that wishes to proceed with its accession to this Code should sign (but not date) both counterparts of the Accession Agreement, and return them to the Code Administrator.

B1.11 Upon return to the Code Administrator of the two counterparts of the Accession Agreement as envisaged by Section B1.10, the Panel shall procure that (as soon as reasonably practicable thereafter) SECCo:

(a) signs each counterpart on behalf of itself and all the Parties (as it is authorised to do under Section B1.14); and

(b) dates each counterpart with the date of such execution.

B1.12 The Code Administrator shall return one signed and dated counterpart of the Accession Agreement to the Applicant, and retain the other counterpart for the Panel's records.

Accession

B1.13 An Applicant will accede to this Code and become a Party with effect from the date of its executed Accession Agreement. The Code Administrator shall give notice of each Applicant's accession to the Applicant, to each other Party and to the Authority. Such notice will confirm the Applicant's Party Details.

SECCo Authority to enter into Accession Agreements

B1.14 Subject to and in accordance with this Section B1, each Party hereby irrevocably and unconditionally authorises SECCo to execute and deliver, on behalf of such Party, any and all Accession Agreements that are substantially in the form of the Specimen Accession Agreement and that have been signed by an Applicant.

Disputes Regarding Admission

B1.15 Where an Applicant disagrees with any decision of the Code Administrator pursuant to Section B1.8, the Applicant may refer the matter to the Panel for determination.

B1.16 Where an Applicant disagrees with any decision of the Panel made pursuant to Section B1.15, the Applicant may refer the matter to the Authority for its determination, which shall be final and binding for the purposes of this Code.

Party Signifiers

B1.17 On an Applicant acceding to this Code and becoming a Party, the Panel shall as soon as reasonably practicable thereafter issue to it a Party Signifier.

B1.18 The Code Administrator shall notify the DCC of each Party Signifier issued to a Party in accordance with Section B1.17.

RDP Signifiers

B1.19 The Panel shall issue to a Registration Data Provider (other than a Gas Network Party or Electricity Network Party which is deemed to be an RDP, acting in its capacity as such) an RDP Signifier:

(a) as soon as reasonably practicable after receipt of a request from that RDP for it to do so; or

(b) in any event prior to issuing an RDP ID, following receipt of an application from that RDP for it to do so.

B1.20 The Code Administrator shall notify the DCC of each RDP Signifier issued to an RDP in accordance with Section B1.19.

Market Participant Identifiers

B1.21 The following shall apply in respect of the Market Participant Identifiers:

(a) the Panel shall, as soon as reasonably practicable after a person becomes a Party, notify the DCC of the Market Participant Identifiers (if any) by which such person is identified under the UNC and/or BSC, as set out in the Party Details contained in the relevant Accession Agreement;

(b) the Panel shall, as soon as reasonably practicable after a Party notifies any change or addition to such unique identifiers under Section M6 (Party Details), or the Panel otherwise becoming aware of any such change or addition, notify the DCC of such change or addition; and

(c) the DCC shall use the information provided to it under this Section B1.21 to interpret the Registration Data and identify eligibility for Services; subject to Section L16.9 (Supplier of Last Resort).

SECCo

B1.22 The provisions of Sections B1.17 and B1.18 (Party Signifiers) shall apply to SECCo as if it was a Party and as if it had been an Applicant.

B2. DCC, USER AND RDP IDENTIFIERS

Panel: Duty to Obtain MA-S Registry Entries

B2.1 The Panel shall obtain one or more MA-S Registry Entries to the extent necessary for the purpose of establishing and issuing EUI-64 Compliant identifiers for use as User IDs, RDP IDs and/or DCC IDs in accordance with the provisions of this Section B2.

ID Allocation Procedure

B2.2 The Panel shall develop and maintain a document to be known as the "**ID Allocation Procedure**", which shall:

(a) make provision for the Panel to establish and issue Party and RDP Signifiers, each of which must be unique under this Code but which need not be EUI-64 Compliant;

(b) make provision for the Panel to establish EUI-64 Compliant identifiers by the concatenation of:

(i) the assigned value of an MA-S Registry Entry obtained by it; and

(ii) a unique extension identifier created by it;

(c) describe the numbering convention to be used by the Panel for the purpose of creating those unique extension identifiers;

(d) set out the application procedure to be followed by any Party which wishes to be issued with an EUI-64 Compliant identifier for use as a User ID or DCC ID, or by any RDP which wishes to be issued with an EUI-64 Compliant identifier for use as an RDP ID; and

(e) set out the procedure to be followed by the Panel in issuing an EUI-64 Compliant identifier to any Party or RDP for such purposes.

B2.3 In developing the ID Allocation Procedure, the Panel shall act in conjunction with the DCC and such other Parties and RDPs as have indicated a wish to be involved, and shall consult with and have regard to the views of all Parties and RDPs.

B2.4 The Panel shall keep the ID Allocation Procedure under review from time to time, and in particular when requested to do so by any Party or RDP, in order to ensure that it remains fit for purpose. Before making any change to the ID Allocation Procedure the Panel shall consult with and have regard to the views of all Parties and RDPs.

Issue of DCC, User and RDP IDs

B2.5 Where:

(a) the DCC wishes to be issued with an EUI-64 Compliant identifier for use as a DCC ID;

(b) another Party wishes to be issued with an EUI-64 Compliant identifier for use as a User ID; or

(c) an RDP wishes to be issued with an EUI-64 Compliant identifier for use as an RDP ID,

it shall, in accordance with the provisions of the ID Allocation Procedure, apply to the Panel for the issue of that identifier.

B2.6 No Party or RDP may apply to the Panel for the issue of an EUI-64 Compliant identifier other than for one of the purposes specified in Section B2.5.

B2.7 On receiving an application from a Party or RDP in accordance with Section B2.5, the Panel shall issue an EUI-64 Compliant identifier in accordance with the provisions of the ID Allocation Procedure.

Issue of Party and RDP Signifiers

B2.8 The Panel shall issue Party and RDP Signifiers to the Code Administrator from time to time, in accordance with the provisions of the ID Allocation Procedure, for their allocation by the Code

Administrator to new Parties pursuant to Section B1.17 (Party Signifiers) and to RDPs pursuant to Section B1.19 (RDP Signifiers).

Record of Signifiers and IDs Issued

B2.9 The Panel shall:

(a) maintain an up to date record of the Party and RDP Signifiers and the EUI-64 Compliant identifiers issued by it pursuant to this Section B2 (and, where applicable, the mapping between them), and make that record available to all Parties and RDPs; and

(b) notify the DCC of any EUI-64 Compliant identifier that it has issued to:

(i) a Party for use as a User ID and the corresponding Party Signifier of that Party; or

(ii) an RDP for use as an RDP ID and the corresponding RDP Signifier of that RDP.

Network Party Subscriber Obligation

B2.10 Each Electricity Network Party shall, as soon as reasonably practicable after its accession to this Code, ensure that it becomes a Subscriber for those Organisation Certificates which pertain to it and that are required by Responsible Suppliers for the purposes of complying with their obligations under Clause 5 (Post-Commissioning Obligations in Relation to SMETS2+ Devices) and Clause 6 (Post Commissioning Obligations in Relation to SMETS1 Devices) of the Inventory Enrolment and Decommissioning Procedures.

B2.11 No Gas Network Party shall become a Subscriber for Organisation Certificates unless it also intends to become a User.

C GOVERNANCE

C1. SEC OBJECTIVES

General SEC Objectives

C1.1 The objectives of this Code otherwise than in respect of the Charging Methodology are set out in Condition 22 of the DCC Licence (such objectives being the **General SEC Objectives**). For ease of reference, the General SEC Objectives are set out below using the terminology of this Code (but in the case of any inconsistency with the DCC Licence, the DCC Licence shall prevail):

(a) the first General SEC Objective is to facilitate the efficient provision, installation, and operation, as well as interoperability, of Smart Metering Systems at Energy Consumers' premises within Great Britain;

(b) the second General SEC Objective is to enable the DCC to comply at all times with the General Objectives of the DCC (as defined in the DCC Licence), and to efficiently discharge the other obligations imposed upon it by the DCC Licence;

(c) the third General SEC Objective is to facilitate Energy Consumers' management of their use of electricity and gas through the provision to them of appropriate information by means of Smart Metering Systems;

(d) the fourth General SEC Objective is to facilitate effective competition between persons engaged in, or in Commercial Activities connected with, the Supply of Energy;

(e) the fifth General SEC Objective is to facilitate such innovation in the design and operation of Energy Networks (as defined in the DCC Licence) as will best contribute to the delivery of a secure and sustainable Supply of Energy;

(f) the sixth General SEC Objective is to ensure the protection of Data and the security of Data and Systems in the operation of this Code;

(g) the seventh General SEC Objective is to facilitate the efficient and transparent administration and implementation of this Code; and

(h) the eighth General SEC Objective is to facilitate the establishment and operation of the Alt HAN Arrangements.

Transition Objective

C1.2 As provided for in Condition 22 of the DCC Licence, during the period prior to the Completion of Implementation, the General SEC Objectives must be read and given effect (so far as it is possible to do so) in a way that is compatible with achieving the Transition Objective.

Charging Objectives

C1.3 The objectives of this Code in respect of the Charging Methodology only (such objectives being the Charging Objectives) comprise the "First Relevant Policy Objective", the "Second Relevant Policy Objective" and the "Third Relevant Policy Objective" as set out in Condition 18 of the DCC Licence. For ease of reference, the First Relevant Policy Objective, the Second Relevant Policy Objective and the Third

Relevant Policy Objective are set out in Sections C1.4, C1.5 and C1.6 using the terminology of this Code (but in the case of any inconsistency with the DCC Licence, the DCC Licence shall prevail).

C1.4 The First Relevant Policy Objective:

(a) applies in respect of Charges (other than Charges for Elective Communications Services); and

(b) requires the Charging Methodology to ensure that such Charges do not distinguish (whether directly or indirectly):

(i) between Energy Consumers at Domestic Premises in different parts of Great Britain; or

(ii) between Energy Consumers at Designated Premises in different parts of Great Britain.

C1.5 The Second Relevant Policy Objective applies in relation to SMETS1 Meters. The Second Relevant Policy Objective is that, subject to compliance with the First Relevant Policy Objective, the Charging Methodology must (other than in respect of Elective Communication Services) (in each of the following cases, as far as is reasonably practicable in all of the circumstances of the case, having regard to the costs of implementing the Charging Methodology):

(a) result in Charges that are the same for SMETS1 Meters as they are for Smart Metering Systems, save that no Charges for Communications Hub Services will apply to SMETS1 Meters;

(b) notwithstanding (a) above (where the Costs of Communications for a SMETS1 Meter exceeds the Costs of Communications for a Smart Metering System, and where an Original Supplier for the Energy Supplier Contract relating to that SMETS1 Meter is (and has at all times since the adoption of the Energy Supplier Contract been) a supplier of electricity and/or gas to the premises at which that SMETS1 Meter is installed), result in Charges that ensure that the excess Costs of Communications are recovered from the Original Supplier from time to time (in addition to the Charges referred to in (a) above),

and, for the purposes of this Section C1.5, the terms "**SMETS1 Meters**", "**Costs of Communications**", "**Original Supplier**" and "**Energy Supplier Contract**" shall have the meaning given to those terms in the DCC Licence.

C1.6 The Third Relevant Policy Objective is that, subject to compliance with the First and Second Relevant Policy Objectives, the Charging Methodology must result in Charges that:

(a) facilitate effective competition in the Supply of Energy (or its use) under the Electricity Act and the Gas Act;

(b) do not restrict, distort, or prevent competition in Commercial Activities that are connected with the Supply of Energy under the Electricity Act and the Gas Act;

(c) do not deter the full and timely installation by Energy Suppliers of Smart Metering Systems at Energy Consumers' premises in accordance with their obligations under the Energy Supply Licence; and

(d) do not unduly discriminate in their application and are reflective of the costs incurred by the DCC, as far as is reasonably practicable in all of the circumstances of the case, having regard to the costs of implementing the Charging Methodology.

C1.7 The Charging Methodology will achieve the Third Relevant Policy Objective if it is compliant with the provisions of Section C1.6 in the round, weighing them as appropriate in each particular case.

C2. PANEL

Establishment of the Panel

C2.1 The Panel is hereby established. The Panel shall:

(a) pursue the objectives, undertake the duties, and have the powers, set out in Sections C2.2 to C2.4;

(b) be composed of the Panel Members described in Section C3 (Panel Members), some of whom will be elected in accordance with Section C4 (Elected Members); and

(c) conduct its activities in accordance with the procedures set out in Section C5 (Proceedings of the Panel).

Panel Objectives

C2.2 The Panel shall, in all its activities, always act in a manner designed to achieve the following objectives (the **Panel Objectives**):

(a) that this Code is given full and prompt effect in accordance with its terms and conditions;

(b) that this Code is given effect in such a manner as will facilitate achievement of the SEC Objectives;

(c) that this Code is given effect in a fair manner without undue discrimination between the Parties or any classes of Party; and

(d) that the Panel conducts its affairs in an open and transparent manner.

Panel Duties

C2.3 Without prejudice to any other tasks, duties or obligations imposed on the Panel in this Code, the Panel shall, subject to and in accordance with the other provisions of this Code:

(a) oversee the process by which Applicants apply to become a Party, as set out in Section B (Accession);

(b) manage the Code Administrator and Secretariat, and oversee their performance;

(c) develop, consult upon, and report upon its performance against three-year budgets and work plans in accordance with Section C8 (Panel Costs and Budgets);

(d) oversee and co-ordinate the process for assessing Draft Proposals and Modification Proposals, and implement successful Modification Proposals, each as set out in Section D (Modification Process);

(e) manage and co-ordinate arrangements for the resolution of certain Disputes under or in relation to this Code, as set out in Section M7.3 (Reference to the Panel or its Sub-Committees);

(f) manage and co-ordinate the suspension of Parties' rights under this Code, as set out in Section M8 (Suspension, Expulsion and Withdrawal);

(g) manage and co-ordinate the withdrawal or expulsion of Parties from this Code, as set out in Section M8 (Suspension, Expulsion and Withdrawal);

(h) by no later than 30 Working Days following the end of each Regulatory Year prepare and publish a report on the implementation of this Code and the activities of the Panel during that Regulatory Year, including so as to evaluate whether this Code continues to meet the SEC Objectives (and in respect of the Alt HAN Arrangements the Panel shall be entitled to rely on and report any information provided to it by the Alt HAN Forum for that purpose);

(i) at the written request of the Authority at any time, undertake a review of such parts of this Code as the Authority may specify to evaluate whether this Code continues to meet the SEC Objectives;

(j) at the written request of the Authority, collect and provide to the Authority (or publish in such manner as the Authority may direct) such information regarding the SEC Arrangements as the Authority may reasonably request (and each Party shall provide to the Panel such information as the Panel reasonably requires in order to enable the Panel to comply with any such request of the Authority);

(k) hold a general meeting during the month of July each year, which each Panel Member will (subject to unforeseen circumstances) attend, at which a representative of each Party shall be entitled to attend and speak, and at which the Panel will endeavour to answer any reasonable questions submitted to the Secretariat in advance of the meeting;

(l) establish (and, where appropriate, revise from time to time) joint working arrangements with the panels, committees and administrators responsible for the governance and operation of other Energy Codes, in order to facilitate the timely:

    (i) identification, co-ordination, making and implementation of changes to other Energy Codes consequent on a Draft Proposal or Modification Proposal (and vice versa); and

    (ii) identification and coordinated resolution of Disputes and disputes under other Energy Codes (in circumstances where there is an interaction between the Dispute and one or more disputes under the other Energy Codes);

(m) establish joint working arrangements with the Information Commissioner pursuant to which the Panel shall notify the Information Commissioner of matters in which the Panel believes the Information Commissioner may have an interest; and

(n) periodically commission a review of the effectiveness of the End-to-End Technical Architecture and the Business Architecture by the Technical Architecture and Business Architecture Sub-Committee, as further described in Section F1 (Technical Architecture and Business Architecture Sub-Committee).

Panel Powers

C2.4 Without prejudice to any other rights or powers granted to the Panel in this Code, the Panel shall, subject to and in accordance with the other provisions of this Code, have the power to:

(a) appoint and remove the Code Administrator and the Secretariat in accordance with Section C7 (Code Administrator, Secretariat and SECCo);

(b) appoint and remove professional advisers;

(c) consider, approve and authorise the entering into by SECCo of contracts in accordance with Section C7 (Code Administrator, Secretariat and SECCo);

(d) constitute Sub-Committees in accordance with Section C6 (Sub-Committees);

(e) consider, approve and authorise the licensing, sub-licensing, or any other manner of dealing with the Intellectual Property Rights in the SEC Materials, for any use which does not hinder, delay or frustrate, in any way whatsoever, the SEC Objectives;

(f) direct SECCo to become a Subscriber for IKI Certificates, on behalf of the Panel and for the purpose of Digitally Signing the Central Products List; and

(g) do anything necessary for, or reasonably incidental to, the discharge of its duties under this Code.

C3. PANEL MEMBERS

Panel Composition

C3.1 The Panel shall be composed of the following categories of persons (each a **Panel Member**, and the Panel Members referred to in Sections C3.1(a) to (e) being the **Elected Members**):

(a) two persons elected by the Large Supplier Parties;

(b) two persons elected by the Small Supplier Parties;

(c) one person elected by the Electricity Network Parties;

(d) one person elected by the Gas Network Parties;

(e) two persons elected by the Other SEC Parties;

(f) one person nominated by the DCC in accordance with Section C3.3 (the **DCC Member**);

(g) two persons nominated in accordance with Section C3.4 (the **Consumer Members**);

(h) one person appointed in accordance with Section C3.5 (the **Panel Chair**); and

(i) any additional person appointed by the Panel Chair in accordance with Section C3.6.

C3.2 Each Panel Member must be an individual (and cannot be a body corporate, association or partnership). No one person can hold more than one office as a Panel Member.

DCC Member

C3.3 The DCC Member shall be one person nominated by the DCC by notice to the Secretariat. The DCC may replace such person from time to time by prior notice to the Secretariat.

Consumer Members

C3.4 The Consumer Members shall be two persons nominated by Citizens Advice or Citizens Advice Scotland by notice to the Secretariat from time to time. Citizens Advice or Citizens Advice Scotland may replace each such person from time to time by prior notice to the Secretariat.

Appointment of the Panel Chair

C3.5 The Panel Chair shall be appointed in accordance with such process as the Panel may determine, as modified from time to time by the Panel; provided that such process as modified must be designed to ensure that:

(a) the candidate selected is sufficiently independent of any particular Party or class of Parties;

(b) the appointment is conditional on the Authority approving the candidate;

(c) the Panel Chair is appointed for a three-year term (following which he or she can apply to be re-appointed);

(d) the Panel Chair is remunerated at a reasonable rate;

(e) the Panel Chair's appointment is subject to Section C3.8 and terms equivalent to those set out in Section C4.6 (Removal of Elected Members); and

(f) provision is made for the Panel Chair to continue in office for a reasonable period following the end of his or her term of office in the event of any delay in appointing his or her successor.

Panel Chair Appointee

C3.6 Where at any time:

(a) no person is currently appointed as a Panel Member pursuant to this Section C3.6; and

(b) the Panel Chair (having consulted with the other Panel Members) considers that there is a class or category of person having an interest in the SEC Arrangements whose interests are not adequately represented in the composition of the Panel at that time, and whose interests would be better represented if a particular person were appointed as an additional Panel Member,

the Panel Chair may (having consulted with the other Panel Members) appoint that particular person as a Panel Member by notice to the Secretariat. The Panel Chair may (having consulted with the other Panel Members), at any time thereafter by notice to the Secretariat, remove that person from the office of Panel Member.

Duties of Panel Members

C3.7 A person appointed as Panel Member, when acting in that capacity, shall:

(a) act independently, not as a delegate, and without undue regard to the interests, of any Related Person;

(b) exercise reasonable skill and care to the standard reasonably expected of a director of a company under the Companies Act 2006; and

(c) act in a manner designed to facilitate the performance by the Panel of its duties under this Code.

Panel Member Confirmation

C3.8 Each Panel Member must confirm in writing to SECCo (for the benefit of SECCo and each Party) that that person:

(a) agrees to act as a Panel Member in accordance with this Code, including the requirements of Section C3.7; and

(b) agrees to accept appointment as a director of SECCo, and to act in such capacity in accordance with this Code; and

(c) will be available as reasonably required throughout his or her term of office, both to attend Panel meetings and to undertake work outside those meetings as may reasonably be required,

and must further complete any and all forms required to be completed by law in order for that person to become a director of SECCo.

C3.9 The appointment of a person who would otherwise be a Panel Member shall lapse (and the relevant office shall become vacant) if that person does not comply with the requirements of Section C3.8 within 20 Working Days after a request from the Secretariat to do so.

Notification of Related Persons

C3.10 Each Panel Member shall, at the time of his appointment and upon any relevant change in circumstance, disclose, in writing to the Panel, the name of each Related Person who is a Party, a DCC Service Provider or is otherwise likely to be materially affected by the SEC Arrangements (other than in the capacity of Energy Consumer).

C3.11 Without prejudice to the generality of Section C3.10, where a Panel Member changes employer, the Panel Member shall (as soon as reasonably practicable after such change) notify the Secretariat of such change in writing. The Secretariat shall then notify the Parties of such change in employer.

Protections for Panel Members and Others

C3.12 SECCo shall indemnify, and keep indemnified:

(a) each Panel Member (whether as a Panel Member or as a director of SECCo);

(b) each Reserve (whether acting as an Alternate or otherwise);

(c) each person who serves on a Sub-Committee or Working Group; and

(d) each Party, or an Affiliate of a Party, as employer of any person referred to in Sections C3.12(a) to (c),

from and against any and all costs (including legal costs), charges, expenses, damages or other liabilities properly incurred or suffered by that person or employer in relation to the exercise of the person's powers duties or responsibilities under this Code, including where such powers duties or responsibilities are exercised negligently. The persons and employers shall be entitled to enforce their rights under this Section C3.12 pursuant to Section M11.5 (Third Party Rights).

C3.13 The indemnity set out in Section C3.12 shall not apply to any costs, charges, expenses, damages or other liabilities that are:

(a) costs and expenses expressly stated to be incapable of recovery by the Panel under Section C8 (Panel Costs and Budgets); or

(b) suffered or incurred or occasioned by the wilful default, fraud or bad faith of the relevant person.

C4. ELECTED MEMBERS

Elected Members

C4.1 The Elected Members shall be elected in accordance with the process set out in Section C4.2. Each Elected Member shall serve as a Panel Member until his or her retirement in accordance with Section C4.4, or until he or she is removed from office in accordance with Section C3.9, C4.5 or C4.6.

Election of Elected Members

C4.2 The process set out in this Section C4.2 shall apply in respect of the election of each Elected Member. This process shall apply in respect of Elected Member vacancies arising by virtue of a Panel Member's retirement in accordance with Section C4.4 (a **Scheduled Election**), or a Panel Member being removed from office in accordance with Section C3.9, C4.5 or C4.6 (an **Interim Election**). In each case, the following process shall apply:

(a) each Elected Member is to be elected by a Party Category as described in Section C3.1;

(b) each Voting Group within a Party Category is entitled to cast one vote in the election of the Panel Member(s) to be elected by that Party Category;

(c) the Secretariat shall publish on the Website and send to each Party within the relevant Party Category an invitation for nominations for candidates for the role of Elected Member for that Party Category;

(d) in the case of Scheduled Elections, the invitation for nomination of candidates shall be published and sent by the Secretariat at least 35 Working Days ahead of the date on which the relevant Panel Member's term of office expires;

(e) in the case of Interim Elections, the invitation for nomination of candidates shall be published and sent by the Secretariat by no later than 5 Working Days after the date on which the relevant Panel Member was removed from office;

(f) the invitation for nomination of candidates shall request nominations within 15 Working Days after the date of the invitation;

(g) the eligible candidates for election shall be those persons who are (at the time of their nomination) capable of becoming and remaining Panel Members in accordance with Sections C3.2 and C4.6, and whose nominations (whether nominated by themselves or a third party) are received by the Secretariat within the period of time set out in the request for nominations;

(h) where the Secretariat receives a nomination for a candidate that the Secretariat does not consider to be an eligible candidate in accordance with Section C4.2(g), the Secretariat shall notify that person that this is the case as soon as reasonably practicable after receipt of the nomination (and, in any event, by no later than 2 Working Days following the expiry of the period of time set out in the request for nominations);

(i) where a candidate disputes the Secretariat's notification under Section C4.2(h), the candidate shall have 2 Working Days following receipt of such notification to refer the matter to the Panel Chair for final determination (which determination shall be made by the Panel Chair by no later than 5 Working Days following the expiry of the period of time set out in the request for nominations);

(j) 6 Working Days following the expiry of the period of time set out in the request for nominations, the Secretariat shall give notice to each Party within the relevant Party Category of the names of each eligible candidate (together with any supporting information provided to the Secretariat with his or her nomination);

(k) at the same time as the Secretariat issues such notice, where there are more eligible candidates for a Party Category than there are positions to be filled as Elected Members for that Party Category, the Secretariat shall invite the Voting Groups comprising that Party Category to vote for their preferred eligible candidate;

(l) each such Voting Group shall be entitled to cast one vote, and shall cast such vote by means of a system established by the Panel which ensures that each Voting Group casts only one vote, and which allows 10 Working Days following the invitation pursuant to Section C4.2(k) for such vote to be cast;

(m) the successful candidate or candidates elected as a result of the votes cast in accordance with this Section C4.2 shall be determined in accordance with Section C4.3;

(n) the Secretariat shall not publish details of the votes cast by each Voting Group, but shall disclose such details to the Panel Chair for scrutiny;

(o) as soon as reasonably practicable following the election of an Elected Member in accordance with this Section C4.2, the Secretariat shall publish on the Website and notify each Party of the identity of the person who has been so elected; and

(p) each person elected as a Panel Member in accordance with this Section C4.2 shall commence his or her office as a Panel Member: (i) in the case of Scheduled Elections, simultaneously with the retirement of the relevant Panel Member; or (ii) in the case of Interim Elections, simultaneously with the notification by the Secretariat pursuant to Section C4.2(o).

C4.3 As a result of the process set out in Section C4.2:

(a) where there are the same number of eligible candidates for a Party Category as there are positions to be filled as Elected Members for that Party Category, all of the eligible candidates shall be elected as Elected Members;

(b) where there are more eligible candidates for a Party Category than there are positions to be filled as Elected Members for that Party Category, the eligible candidate(s) that received the most votes in accordance with Section C4.2(l) shall be elected as Elected Members (and, in the case of a tie, the

Secretariat shall determine the Elected Member by drawing lots, to be witnessed by the Panel Chair); or

(c) where there are fewer eligible candidates for a Party Category than there are positions to be filled as Elected Members for that Party Category (including where there are no eligible candidates), the Authority will (at its discretion) be entitled to nominate an Elected Member for that Party Category. Where this Section C4.3(c) applies, the Panel shall be entitled (at any time thereafter) to determine that a further Interim Election should be held in accordance with Section C4.2 in respect of that Party Category.

Retirement of Elected Members

C4.4 Subject to earlier removal from office of an Elected Member in accordance with Section C3.9, C4.5 or C4.6 and without prejudice to his or her ability to stand for re- election, each Elected Member shall retire (at which point his or her office shall become vacant) as follows:

(a) not used;

(b) the Elected Members elected in accordance with this Section C4.2, shall retire two years after the date on which they first took office; and

(c) any Elected Member nominated by the Authority pursuant to Section C4.3(c), shall retire on the Authority determining (at its discretion) that such person should be removed from office, or on the successful election of a replacement Elected Member in an election pursuant to Section C4.3(c).

Removal of Elected Members

C4.5 An Elected Member may:

(a) resign his or her office by 10 Working Days’ notice in writing to the Panel Chair;

(b) be removed from office by the Panel Chair on notice to the Panel if the Elected Member fails to attend (either in person or via his or her Alternate) at least 50% of the Panel meetings held in any period of 12 months; or

(c) be removed from office by the other Panel Members (acting unanimously) if such other Panel Members consider that the Elected Member is in breach of the confirmation given by that Elected Member pursuant to Section C3.8 (Panel Member Confirmation).

C4.6 An Elected Member shall automatically be removed from office if he or she:

(a) dies;

(b) is admitted to hospital in pursuance of an application under the Mental Health Act 1983 or the Mental Health (Care and Treatment) (Scotland) Act 2003, or an order is made by a court with competent jurisdiction in matters concerning mental disorder for his detention or for the appointment of a receiver, curator bonis or other person with respect to his property or affairs;

(c) becomes bankrupt or makes any arrangement or composition with his creditors;

(d) becomes prohibited by law from being a director of a company under the Companies Act 2006; and/or

(e) is convicted of an indictable criminal offence.

C5. PROCEEDINGS OF THE PANEL

Meetings of the Panel

C5.1 The Panel shall hold meetings with such frequency as it may determine or the Panel Chair may direct, but in any event shall meet when necessary to meet its responsibilities under Section D (Modification Process) and at least once every two months.

C5.2 The location and timing of each meeting shall be determined by the Panel. Panel Members shall endeavour to attend each meeting in person, but attendance by telephone conference or other technological means shall be permitted (provided that each of the Panel Members attending the meeting acknowledges that he or she can communicate with each other).

C5.3 Subject to the other provisions of this Code, the Panel may regulate the conduct of its meetings as it sees fit.

Quorum

C5.4 No business shall be transacted at any meeting of the Panel unless a quorum is present at that meeting. The quorum for each Panel meeting shall be one half of all Panel Members appointed at the relevant time, at least one of whom must be the Panel Chair.

Meeting Notice and Papers

C5.5 Each meeting that the Panel determines, or the Panel Chair directs, is to be held shall be convened by the Secretariat. Such meeting shall be convened on at least 5 Working Days' advance notice (or such shorter period as the Panel may approve). Such notice must be given to:

(a) the Panel Members (and any appointed Alternates);

(b) each of the persons referred to in Section C5.13;

(c) the Parties; and

(d) any other person that the Panel determines, or the Panel Chair directs, should be invited to the meeting.

C5.6 The notice of each Panel meeting shall contain or be accompanied by the following:

(a) the time, date and location of the meeting;

(b) the arrangements for those wishing to attend the meeting by telephone conference or other technological means; and

(c) an agenda and supporting papers.

C5.7 The accidental omission to give notice of a meeting to, or the non-receipt of notice of a Panel meeting by, a person entitled to receive notice shall not invalidate the proceedings of that meeting.

Panel Chair

C5.8 The Panel Chair shall preside at every meeting of the Panel. If the Panel Chair is unable to attend a Panel meeting, the Panel Chair shall ensure that his or her Alternate attends the meeting as Panel Chair.

C5.9 The Panel Chair shall not be entitled to vote unless there is a deadlock, in which case the Panel Chair shall have the casting vote.

Voting

C5.10 Subject to Section C5.9, each Panel Member shall be entitled to attend, and to speak and vote at, every meeting of the Panel.

C5.11 All decisions of the Panel shall be by resolution. In order for a resolution of the Panel to be passed at a meeting, a simple majority of those Panel Members voting at that meeting must vote in favour of that resolution.

C5.12 A resolution in writing signed by or on behalf of all the Panel Members shall be as valid and effective as if it had been passed at a meeting of the Panel duly convened and held. Such a resolution may be signed in any number of counterparts.

Attendance by other persons

C5.13 One representative from each of the following persons shall be entitled to attend and speak (but not vote) at any meeting of the Panel:

(a) the Secretary of State;

(b) the Authority; and

(c) any other person that the Panel determines, or the Panel Chair directs, should be invited to attend.

C5.14 Any Party shall be entitled to send a representative to attend a Panel meeting provided that Party gives the Secretariat at least 3 Working Days' notice in advance of such meeting (or such shorter period of notice as the Panel Chair may approve). Such a representative shall be entitled to attend and (at the Panel Chair's invitation) speak at (but in no circumstances vote at) the meeting.

C5.15 The Panel Chair may (at his or her discretion on grounds of confidentiality) exclude from any part of a Panel meeting persons admitted pursuant to Section C5.13(c) or C5.14.

Minutes of Panel Meetings

C5.16 The Secretariat shall, following each Panel meeting (and in any event at or before the next Panel meeting), circulate copies of the minutes of that meeting to each person who was entitled to receive a notice of that meeting. The Panel may determine that certain parts of a meeting are confidential, in which case those matters will not be included in the minutes circulated to persons other than the Panel, the Secretary of State and the Authority.

C5.17 If any Panel Member disagrees with any item of the minutes, he shall notify the Secretariat of those items with which he or she disagrees, and the Secretariat shall incorporate those items upon which there is disagreement into the agenda for the next following meeting of the Panel.

C5.18 The Secretariat shall maintain a record of all resolutions voted on by the Panel, indicating how each Panel Member voted on each resolution, and shall make such record available on request to any Party.

Alternates

C5.19 Each Panel Member may, from time to time by notice in writing to the Secretariat, appoint another natural person to act as his or her alternate (an **Alternate**). The Panel Chair must appoint a person to act as his or her Alternate.

C5.20 Each such Alternate must, before his or her appointment as such can become valid, have provided the confirmations referred to in Sections C3.8(a) and (c) (Panel Member Confirmation).

C5.21 Where a Panel Member does not attend at a Panel meeting, the Panel Member's Alternate shall be entitled to attend (and count, in his capacity as Alternate, towards the quorum at) that meeting, and to exercise and discharge all the functions, powers and duties of the Panel Member at that meeting.

C5.22 Each Panel Member may, by notice in writing to the Secretariat, remove or replace the person appointed from time to time by that Panel Member as his or her Alternate. An Alternate shall immediately cease to be an Alternate on the occurrence of any of the events set out in Section C4.5 (Removal of Elected Members) in respect of the Alternate. Where an Alternate's appointor ceases to be a Panel Member for any reason, the Alternate's role as such shall also cease.

C5.23 Unless the context otherwise requires, any reference in this Code to a Panel Member shall be construed as including a reference to that Panel Member's Alternate.

Conflicts of interest

C5.24 Given the duty of each Panel Member to act independently, as set out in C3.7 (Duties of the Panel), conflicts of interest should not regularly arise.

C5.25 Notwithstanding Section C5.24, where a decision of the Panel will have particular consequences for a particular Party or class of Parties, each Panel Member shall consider whether that decision presents a conflict of interest (whether because such Party or Parties comprise Related Persons of the Panel Member or otherwise).

C5.26 Where a Panel Member considers that a decision does present a conflict of interest, the Panel Member shall absent him or herself from the Panel meeting for that decision and abstain from the vote regarding that decision. Furthermore, where the Panel Chair considers that a decision does present a conflict of interest for a Panel Member, the Panel Chair may require the Panel Member to absent him or herself from the Panel meeting for that decision and to abstain from the vote regarding that decision.

C6. SUB-COMMITTEES

Sub-Committees

C6.1 The Panel may establish committees (**Sub-Committees**) for the purposes of doing or assisting the Panel in doing anything to be done by the Panel pursuant to this Code. The Panel shall establish those Sub-Committees expressly provided for in this Code.

C6.2 The Panel may establish a Sub-Committee on a standing basis or for a fixed period or a finite purpose.

C6.3 The Panel may decide that any Sub-Committee (other than one whose establishment is expressly provided for in this Code) is to be dissolved. Those Sub-Committees expressly provided for in this Code are to remain established for so long as they are provided for in this Code.

C6.4 Subject to Section C6.5, the Panel may delegate to any Sub-Committee such of the duties, powers and functions of the Panel as the Panel may specify. The Panel shall delegate to any Sub-Committee expressly provided for in this Code all of the duties, powers, and functions of the Panel relating to the functions of that Sub-Committee described in this Code.

Working Groups

C6.5 The Panel may not establish Sub-Committees to undertake the functions expressly reserved to Working Groups under Section D (Modification Process). Working Groups are to be subject to the requirements of Section D6 (Refinement Process), which may impose requirements by reference to this Section C6.

Membership

C6.6 Each Sub-Committee expressly provided for in this Code shall be composed of such persons as are determined in accordance with the provisions of this Code (if any) that prescribe such membership (and otherwise in accordance with Section C6.7).

C6.7 Subject to Section C6.6:

(a) each Sub-Committee shall be composed of such persons of suitable experience and qualifications as the Panel shall decide and as are willing to serve thereon, and which may include any Panel Member;

(b) before establishing each Sub-Committee, the Panel shall invite (by such means as it considers appropriate) applications from individuals who wish to serve on that Sub-Committee;

(c) once a Sub-Committee has been established, the Panel may admit such additional persons to, or remove any person from, that Sub-Committee as the Panel considers appropriate (including on the application of any Party or any member of the Sub-Committee).

C6.8 Each person serving on a Sub-Committee shall, when acting in that capacity:

(a) act independently, not as a delegate, and without undue regard to the interests, of any Related Person; and

(b) act in a manner designed to facilitate the performance by the Panel of its duties under this Code.

Member Confirmation

C6.9 Unless the Panel otherwise directs, a person who is to serve on a Sub-Committee shall not do so unless he or she has first provided a written confirmation to SECCo (for the benefit of SECCo and each Party) that that person:

(a) agrees to serve on the Sub-Committee in accordance with this Code, including the requirements of Section C6.8; and

(b) will be available as reasonably required throughout his or her term of office, both to attend Sub-Committee meetings and to undertake work outside those meetings as may reasonably be required.

Terms of Reference and Procedural Requirements

C6.10 The Panel shall set out in writing the duties, powers, and functions of the Panel that it has delegated to each Sub-Committee. The Panel shall also specify in the same document the terms of reference and procedural rules that are to be followed by the Sub-Committee (which may be revised from time to time by the Panel); provided that, in the case of Sub-Committees expressly provided for in this Code, the Panel must specify terms of reference and procedural rules consistent with the requirements (if any) expressly set out in this Code.

C6.11 Save to the extent otherwise specified by the Panel in accordance with Section C6.10, each Sub-Committee shall conduct its business in accordance with the requirements applying to the Panel in accordance with Section C5 (Proceedings of the Panel).

C6.12 No Sub-Committee may further delegate any of its duties, powers and functions unless expressly authorised to do so by the terms of reference and procedural rules specified in accordance with Section C6.10.

Decisions of Sub-Committees

C6.13 Resolutions of Sub-Committees shall only have binding effect as decisions of the Panel if the Panel has formally delegated the decision-making powers to the Sub- Committee.

C6.14 The Panel shall be deemed to have delegated its decision-making powers to each Sub- Committee expressly provided for in this Code, insofar as such decision-making powers relate to the functions of the Sub-Committee. The delegation of decision- making powers to any other Sub-Committee shall require the unanimous agreement of all Panel Members at the meeting at which the decision to delegate such powers is agreed.

C6.15 For the avoidance of doubt, the delegation to a Sub-Committee of any duties, powers and functions of the Panel shall not relieve the Panel of its general responsibility to ensure that such duties, powers and functions are exercised in accordance with this Code.

C7. CODE ADMINISTRATOR, SECRETARIAT AND SECCO

Code Administrator

C7.1 The Panel may, from time to time, appoint and remove, or make arrangements for the appointment and removal of, one or more persons to be known as the **Code Administrator**.

C7.2 The Code Administrator shall perform those tasks and functions expressly ascribed to it under this Code, and any other tasks and functions as the Panel may assign to the Code Administrator from time to time. In particular, the Code Administrator shall:

(a) comply with the Code Administration Code of Practice and perform its tasks and functions in a manner consistent with the Code Administration Code of Practice Principles (provided that the requirements of this Code shall apply in the event of any inconsistencies between this Code and the requirements of the Code Administration Code of Practice);

(b) in conjunction with the other persons named as code administrators in the Code Administration Code of Practice, review and where appropriate propose to the Authority that amendments be made to the Code Administration Code of Practice (subject always to the Authority's approval of those amendments);

(c) report to the Panel on any inconsistencies between this Code and the requirements of the Code Administration Code of Practice;

(d) support the process by which Applicants apply to become a Party, as set out in Section B (Accession);

(e) support the process for Modifications, as set out in Section D (Modification Process);

(f) facilitate a process whereby Parties can submit a Draft Proposal to the Code Administrator to have that potential variation developed, refined and discussed prior to the Party deciding whether to formally progress this as a Modification Proposal (whether through the Change Board or another forum);

(g) support the process by which Parties become Users, as set out in Section H1 (User Entry Process);

(h) act as a critical friend in providing assistance and support to Parties (and prospective Parties) in relation to the other tasks and functions to be performed by the Code Administrator, with a view to providing particular assistance and support to small Parties and the Consumer Members;

(i) without prejudice to the generality of Section C7.2(i), provide support and assistance to the Proposer of a Draft Proposal, including assistance in understanding this Code so as to properly frame any subsequent Modification Proposal;

(j) advise the Panel (and Sub-Committees and Working Groups) as to, and in respect of, the matters of which it is necessary or appropriate that the Panel (or the Sub-Committee or Working Group) should be aware in order to discharge their functions in accordance with this Code; and

(k) provide or procure such information in connection with the implementation of this Code as the Panel may require.

C7.3 The Panel shall be responsible for ensuring that the Code Administrator undertakes its tasks and functions in respect of this Code. In particular, the Panel shall ensure that the arrangements under which the Code Administrator is appointed oblige the Code Administrator to undertake such tasks and functions on terms no less onerous than those provided for by this Code.

C7.4 Subject to the other requirements of this Section C7, the Code Administrator shall be appointed by the Panel on such terms and conditions and in return for such remuneration as the Panel sees fit.

C7.5 In no event shall the Code Administrator be a Party, an Affiliate of a Party, an employee of a Party, an employee of an Affiliate of a Party, a DCC Service Provider, an Affiliate of a DCC Service Provider, an employee of a DCC Service Provider, or an employee of an Affiliate of a DCC Service Provider.

Secretariat

C7.6 The Panel may, from time to time, appoint and remove, or make arrangements for the appointment and removal of, one or more persons to be known as the **Secretariat**.

C7.7 The Secretariat shall perform those tasks and functions expressly ascribed to it under this Code, and any other tasks and functions as the Panel may assign to the Secretariat from time to time. In particular, the Secretariat shall:

(a) support the election of Elected Members, as set out in Section C4 (Elected Members);

(b) support the proceedings of the Panel (and Sub-Committees and Working Groups), as set out in Section C5 (Proceedings of the Panel);

(c) provide or procure such facilities and services in connection with the operation of the Panel (and Sub-Committees and Working Groups) as the Panel may require;

(d) maintain each Party's Party Details, as set out in Section M6 (Party Details);

(e) procure the creation, hosting and maintenance of the Website; and

(f) make an accurate and up-to-date copy of this Code available on the Website.

C7.8 The Panel shall be responsible for ensuring that the Secretariat undertakes its tasks and functions in respect of this Code. In particular, the Panel shall ensure that the arrangements under which the Secretariat is appointed oblige the Secretariat to undertake such tasks and functions on terms no less onerous than those provided for by this Code.

C7.9 Subject to the other requirements of this Section C7, the Secretariat shall be appointed by the Panel on such terms and conditions and in return for such remuneration as the Panel sees fit.

C7.10 In no event shall the Secretariat be a Party, an Affiliate of a Party, an employee of a Party, an employee of an Affiliate of a Party, a DCC Service Provider, an Affiliate of a DCC Service Provider, an employee of a DCC Service Provider, or an employee of an Affiliate of a DCC Service Provider.

SECCo

C7.11 SECCo shall be established in accordance with Schedule 4.

C7.12 SECCo shall act as a corporate vehicle in relation to the business of the Panel, including:

(a) entering into any contractual arrangements in order to give effect to any resolution of the Panel which it is necessary or desirable to implement by means of a binding contract; and

(b) becoming a Subscriber for IKI Certificates as directed by the Panel for the purpose of exercising any function of the Panel under this Code.

Market-wide Half-Hourly Settlement Implementation

C7.13 SECCo shall (and the Panel shall ensure that SECCo shall) comply with the obligations expressed to apply to SECCo (either specifically or generically as a category of participant) under section C12 (Market-wide Half-Hourly Settlement Implementation) of the Energy Code known as the Balancing and Settlement Code.

C8. PANEL COSTS AND BUDGETS

General

C8.1 The costs and expenses incurred by (or on behalf of) the Panel in exercising its powers and performing its duties in respect of this Code shall be incurred by SECCo, and the DCC shall provide SECCo with the funds necessary to meet such costs and expenses.

SEC Costs and Expenses

C8.2 The costs and expenses capable of recovery under this Section C8 (the **Recoverable Costs**) shall be all the reasonable costs and expenses incurred:

(a) subject to Section C8.3, by the Panel Members in their capacity as such (including in their capacity as directors of SECCo);

(b) subject to Section C8.3, by those serving on Sub-Committees (but not, for the avoidance of doubt, Working Groups) in their capacity as such;

(c) by SECCo under or in connection with this Code; or

(d) by SECCo under or in connection with contracts that SECCo has entered into in accordance with this Code, including the contracts for:

(i) the appointment of the Code Administrator and the Secretariat;

(ii) the appointment of the Panel Chair;

(iii) the appointment of any person serving on a Sub-Committee expressly provided for in this Code where that person is expressly stated to be remunerated; and

(iv) the appointment of advisers,

(in each case) provided that such costs or expenses are provided for in, or otherwise consistent with, an Approved Budget.

C8.3 Subject to the terms of those contracts referred to in Sections C8.2(d):

(a) each Panel Member and each person serving on a Sub-Committee shall be entitled to recover all reasonable travel expenses properly incurred by them in their roles as such (and the Panel shall establish a policy that sets out guidelines regarding what constitutes reasonable travel expenses); and

(b) no Panel Member or person serving on a Sub-Committee shall be entitled to a salary in respect of their role as such, or to any payment in respect of time they incur in their role as such.

Reimbursing Panel Members

C8.4 Where a Panel Member or person serving on a Sub-Committee wishes to recover any Recoverable Costs, he or she shall submit evidence of the Recoverable Costs in question to the Panel (or a named person approved by the Panel) for approval. The cost or expense in question shall only be approved to the extent that it is a Recoverable Cost, and only if the evidence is submitted in a timely manner (and in any event on or before the 20th Working Day following the end of the relevant Regulatory Year). Once approved, the evidence of the Recoverable Cost shall be submitted to SECCo for payment.

C8.5 Within 20 Working Days following receipt of evidence of a Recoverable Cost that has been approved in accordance with Section C8.4, SECCo shall pay the relevant amount to the relevant person.

SEC Costs to be Reimbursed by DCC

C8.6 The Recoverable Costs incurred by SECCo shall be reimbursed to SECCo by the DCC.

C8.7 SECCo may periodically invoice the DCC for the Recoverable Costs incurred, or reasonably expected to be incurred, by SECCo; provided that SECCo shall deduct from such Recoverable Costs amounts that SECCo has received by way of Application Fee payments and any amounts that represent previous overpayments by the DCC (due to the inaccuracy of SECCo estimates, or otherwise).

C8.8 The DCC shall pay each invoice submitted by SECCo in accordance with Section C8.7 within 10 Working Days of receipt of such invoice by the DCC.

C8.9 It is acknowledged that the DCC is entitled to recover amounts paid by it to SECCo in accordance with this Section C8 through the Charges (subject to the requirements of the DCC Licence).

C8.10 In the event that the DCC does not pay SECCo in accordance with Section C8.8, and subject to prior approval from the Authority, SECCo may invoice the Parties who hold Energy Licences for the unpaid amount (and those Parties shall pay the invoiced amounts to SECCo as if they were Charges). Where this Section C8.10 applies, the amount to be paid by each Party shall be determined in accordance with a methodology approved by the Authority, and all amounts paid shall be reimbursed by SECCo to the relevant Party (plus interest at the Non-Default Interest Rate) at such time as the Authority may determine.

Draft Budgets and Work Plans

C8.11 The Panel shall, during January of each year, prepare and circulate to all the Parties a draft budget for the next three Regulatory Years commencing thereafter (a **Draft Budget**).

C8.12 Each Draft Budget shall set out the Panel's good-faith estimate of the Recoverable Costs that it anticipates will be incurred (or committed to) during the relevant Regulatory Years, and shall be accompanied by a detailed work plan showing the activities and projects to which the relevant costs and expenses relate. Each Draft Budget must provide for limits (both individually and in the aggregate) on costs and expenses not expressly provided for in the budget which can be incurred without having to amend the budget.

Approval of Budgets

C8.13 In respect of the Draft Budget circulated in January for the next Regulatory Year commencing thereafter, the Panel shall:

(a) arrange for the circulation to all the Parties of the comments received from the Parties regarding the Draft Budget in the 20 Working Days following its circulation;

(b) consider and respond to those comments, and circulate its responses to all the Parties;

(c) to the extent that it considers it appropriate to do so, amend the Draft Budget and/or the accompanying work plan in the light of those comments;

(d) approve the Draft Budget (subject to any such amendments) and publish that budget and the accompanying work plan on the Website; and

(e) specify a date in such publication (being not less than 15 Working Days following the date of publication) from which such budget will (subject to Section C8.14) become the **Approved Budget** for the relevant Regulatory Year.

Appeal of Budget

C8.14 Each of the Parties or Citizens Advice or Citizens Advice Scotland may appeal to the Authority the Panel's approval of a budget as the Approved Budget for a Regulatory Year. Any such appeal will only be validly made if notified to the Authority within 10 Working Days following the publication of such Draft Budget pursuant to Section C8.13(e), and if copied to the Panel. In the event an appeal is validly made, the Panel shall arrange for a copy of the appeal to be circulated to all the Parties, and:

(a) the Authority may give notice that it dismisses the appeal where it considers that the appeal is trivial or vexatious or has no reasonable prospect of success, in which case the budget approved by the Panel shall remain the Approved Budget; or

(b) the Authority may give notice that it will further consider the appeal, in which case the budget approved by the Panel shall remain the Approved Budget pending and subject to any interim directions issued by the Authority, and:

(i) where the Authority determines that the budget approved by the Panel is consistent with the General SEC Objectives, then such budget shall remain the Approved Budget; or

(ii) where the Authority determines that the budget approved by the Panel is not consistent with the General SEC Objectives, then either (as directed by the Authority):

(A) such budget shall be amended in such manner as the Authority may direct, and such budget as so amended will be Approved Budget; or

(B) the Panel shall produce a further Draft Budget and re- commence the process set out in Section C8.13.

Amendments to Budgets

C8.15 The Approved Budget relating to each Regulatory Year may be amended by the Panel from time to time (whether before during or after that Regulatory Year, and including in respect of Recoverable Costs already incurred), provided that the Panel has first:

(a) circulated and invited comments on the proposed amendments in accordance with Section C8.13 as if it were a Draft Budget; and

(b) circulated and considered any comments received on the proposed amendments within 20 Working Days of such circulation on the same basis as is referred to in Section C8.13.

Reports

C8.16 The Panel shall, as soon as is reasonably practicable following the end of each Regulatory Year, produce and circulate to Parties a report on the costs and expenses incurred (or committed to) during that Regulatory Year and the activities and projects to which those costs and expenses relate.

Audit

C8.17 The Panel shall arrange for the monies paid by and to SECCo pursuant to this Section C8 during each Regulatory Year to be audited by a firm of chartered accountants on an annual basis in order to verify whether the requirements of this Section C8 have been met.

C8.18 The Panel shall send a copy of such auditor’s report to all the Parties within 10 Working Days of its receipt by the Panel.

Contents

D MODIFICATION PROCESS

D1. RAISING DRAFT PROPOSALS

Modifications

D1.1 This Code may only be varied in accordance with the provisions of this Section D.

D1.2 Each variation of this Code must commence with a proposal made in accordance with the provisions of this Section D1 (a **Draft Proposal**) or a direction under Section D9A (Authority-Led Variations).

Persons Entitled to Submit Draft Proposals

D1.3 A Draft Proposal may be submitted by any of the following persons (the **Proposer**):

(a) a Party;

(b) Citizens Advice or Citizens Advice Scotland;

(c) any person or body that may from time to time be designated in writing by the Authority for the purpose of this Section D1.3;

(d) the Authority or the DCC acting at the direction of the Authority, but in each case only in respect of variations to this Code which are in respect of a Significant Code Review;

(e) the Secretary of State or the DCC acting at the direction of the Secretary of State, but in each case only in respect of variations to this Code which are intended to protect the security of the End-to-End Smart Metering System (or any part of the End-to-End Smart Metering System);

(f) the Panel (where all Panel Members at the relevant meeting vote unanimously in favour of doing so), but only in respect of variations to this Code which are intended to give effect to:

(i) recommendations contained in a report published by the Panel pursuant to Section C2.3(i) (Panel Duties);

(ii) recommendations contained in a report published by the Code Administrator pursuant to Section C7.2(c) (Code Administrator); and/or

(iii) Fast-Track Modifications (as described in Section D2.8 (Fast-Track Modifications)); and/or

(g) the REC Code Manager and/or the Code Administrator where a Consequential Change to this Code has been identified.

Form of the Draft Proposal

D1.4 The Proposer must submit a Draft Proposal to the Code Administrator.

D1.5 The Code Administrator shall from time to time publish a prescribed form for submitting a Draft Proposal on the Website. The prescribed form must require the provision by the Proposer of all of the information set out in Section D1.7, and any other information that the Panel may reasonably approve.

D1.6 Each Proposer must use the prescribed form when submitting a Draft Proposal.

Content of the Proposal

D1.7 A Draft Proposal must contain the following information:

(a) the name of the Proposer;

(b) the name and contact details of an employee or representative of the Proposer who will act as a principal point of contact in relation to the proposal;

(c) the date on which the proposal is submitted;

(d) a description in sufficient detail of the nature of the proposed variation to this Code and of its intended purpose and effect;

(e) a statement of whether, in the opinion of the Proposer, the Modification Proposal should be a Self-Governance Modification;

(f) a statement of whether the Proposer considers, in the light of any guidance on the topic issued by the Authority from time to time, that the Modification Proposal should be treated as an Urgent Proposal (and, if so, its reasons for so considering);

(g) a statement of whether or not the Modification Proposal is intended to be a Fast- Track Modification;

(h) a statement of the reasons why the Proposer believes that this Code would, if the proposed variation were made, better facilitate the achievement of the SEC Objectives than if that variation were not made;

(i) a statement of whether the Proposer believes that there would be a material impact on Greenhouse Gas Emissions as a result of the proposed variation being made; and

(j) a statement of whether the Proposer believes the Draft Proposal should be submitted directly to the Panel.

Modification Register

D1.8 The Secretariat shall establish and from time to time maintain a register (the **Modification Register**) of all current and past Draft Proposals and Modification Proposals.

D1.9 The Modification Register shall contain, in respect of each Draft Proposal submitted pursuant to this Section D1 and Modification Proposal subsequently raised pursuant to Section D3:

(a) a unique reference number by which the Draft Proposal or Modification Proposal can be identified;

(b) a brief summary of the Modification Proposal and its purpose and effect;

(c) not used;

(d) the stage of the process set out in this Section D that the Draft Proposal or Modification Proposal has reached;

(e) following the Panel's determination pursuant to Section D3 that the Draft Proposal should be progressed as a Modification Proposal:

(i) whether the proposal is a Self-Governance Modification;

(ii) whether the proposal is a Fast-Track Proposal; and

(iii) the timetable applying in respect of the Modification Proposal;

(f) whether the Authority has determined the Modification Proposal to be an Urgent Proposal;

(g) not used;

(h) not used;

(i) once it has been made, the decision of the Panel (in the case of Fast-Track Modifications) or of the Change Board (in the case of all other Modification Proposals); and

(j) such other matters relating to the Draft Proposal or Modification Proposal as the Panel may reasonably determine from time to time.

D1.10 The Secretariat shall ensure that the Modification Register is updated at regular intervals so that the information it contains in relation to each Draft Proposal and Modification Proposal is, so far as is reasonably practicable, accurate and up-to-date.

D1.11 The Secretariat shall ensure that the Modification Register is published on the Website, and that a copy of the Modification Register is sent to each Party at least once every month.

Representations from Parties

D1.12 Each Party shall be free to make written representations from time to time regarding each Draft Proposal or Modification Proposal. Such representations should be made to the Code Administrator in the first instance. The Code Administrator shall:

(a) in the case of Fast-Track Modifications, bring such representations to the attention of the Panel;

(b) in the case of Modifications Proposals (other than Fast-Track Modifications) which are not following the Refinement Process, consider such representations when producing the Modification Report;

(c) in the case of Modifications Proposals (other than Fast-Track Modifications) which are following the Refinement Process, bring such representations to the attention of the relevant Working Group; and

(d) in the case of Draft Proposals, bring such representations to the attention of the Change Sub-Committee.

D2. MODIFICATION PATHS

General

D2.1 Each Modification Proposal will follow one of four modification paths (as described in this Section D2). The modification path to be followed in respect of a Modification Proposal will depend upon the nature of the variation proposed in the Modification Proposal.

D2.2 The Panel's determination (whether under Section D3.12 or subsequently) of whether a Modification Proposal is a Self-Governance Modification shall be conclusive unless and until any contrary determination is made by the Authority in accordance with Section D4 (Authority Determinations).

D2.3 Where the Panel raises a Fast-Track Modification, such Modification Proposal shall be treated as a Fast-Track Modification unless and until any contrary determination is made by the Authority in accordance with Section D4 (Authority Determinations).

Authority-initiated Modification

D2.4 A Draft Proposal submitted:

(a) pursuant to Section D1.3(d) by either the Authority or the DCC at the direction of the Authority;

(b) pursuant to Section D1.3(e) by either the Secretary of State or the DCC at the direction of the Secretary of State,

shall have the status of an **Authority-initiated Modification**.

D2.5 The DCC shall submit a Draft Proposal in respect of any variations:

(a) arising out of a Significant Code Review that the DCC is directed to submit by the Authority;

(b) relating to protecting the security of the End-to-End Smart Metering System (or any part of the End-to-End Smart Metering System) that the DCC is directed to submit by the Secretary of State.

Authority Determined Modifications

D2.6 Unless it is an Authority-initiated Modification, a Modification Proposal that proposes variations to this Code that satisfy one or more of the following criteria shall have the status of an **Authority-initiated Modification**:

(a) the variations are likely to have a material effect on existing or future Energy Consumers;

(b) the variations are likely to have a material effect on competition in the Supply of Energy or Commercial Activities connected with the Supply of Energy;

(c) the variations are likely to have a material effect on the environment, on access to or privacy of Data, on security of the Supply of Energy, and/or on the security of Systems and/or Smart Metering Systems;

(d) the variations are likely to have a material effect on the arrangements set out in Section C (Governance) or this Section D; and/or

(e) the variations are likely to unduly discriminate in their effects between one Party (or class of Parties) and another Party (or class of Parties).

Self-Governance Modification

D2.7 A Modification Proposal that is not an Authority-initiated Modification, an Authority Determined Modification or a Fast Track Modification shall have the status of a **Self- Governance Modification**.

Fast-Track Modifications

D2.8 A Modification Proposal submitted to correct typographical errors or other minor factual inaccuracies or inconsistencies in this Code that do not constitute material changes shall have a status of a **Fast-Track Modification**.

D2A THE CHANGE SUB-COMMITTEE

Establishment of the Change Sub-Committee

D2A.1 The Panel shall establish a Sub-Committee as described in this Section D2A, to be known as the **Change Sub-Committee**. Save as expressly set out in this Section D2A, the Change Sub-Committee shall be subject to the provisions concerning Sub- Committees set out in Section C6 (Sub-Committees).

D2A.2 The Panel may discharge the requirements of Section D2A.1 by allocating the function of the Change Sub-Committee to another Sub-Committee. If the Panel elects to do this, all references to the Change Sub-Committee in this Code shall be treated as references to this other Sub-Committee.

Function of the Change Sub-Committee

D2A.3 The function of the Change Sub-Committee shall be to facilitate the development, refinement and discussion of Draft Proposals prior to their progression as Modification Proposals.

D3. INITIAL ASSESSMENT OF DRAFT PROPOSALS

Invalid Draft Proposals

D3.1 The Code Administrator shall refuse (and may only refuse) to accept the submission of a Draft Proposal that is not submitted:

(a) by a person entitled to submit Draft Proposals in accordance with Section D1.3 (Persons Entitled to Submit Draft Proposals); and/or

(b) in the form, and containing the content, required by Sections D1.6 (Form of the Proposal) and D1.7 (Content of the Proposal).

D3.2 Where the Code Administrator refuses to accept the submission of a Draft Proposal, it shall notify the Panel and the Proposer of that refusal as soon as is reasonably practicable, setting out the grounds for such refusal.

D3.3 Where the Panel is notified that the Code Administrator has refused to accept the submission of a Draft Proposal, the Panel may instruct the Code Administrator to accept the submission of that proposal (and Section D3.4 shall apply as if the Code Administrator had not refused to accept the Modification Proposal).

Initial Comment by the Code Administrator

D3.4 Unless the Code Administrator has refused to accept the submission of the Draft Proposal, the Code Administrator shall, within the time period reasonably necessary to allow the Change Sub-Committee to comply with the time periods set out in Section D3.6 or the Panel to comply with the time periods set out in Section D3.10, submit to the Change Sub-Committee or the Panel as applicable:

(a) each Draft Proposal; and

(b) without altering the Draft Proposal in any way and without undertaking any detailed evaluation of the Draft Proposal, the Code Administrator’s written views on the matters that the Change Sub-

Committee is to consider under Sections D3.7 and D3.8 or Panel is to consider under Sections D3.11 and D3.12.

Initial Consideration by the Change Sub-Committee

D3.5 The Change Sub-Committee shall consider each Draft Proposal that:

(a) has not been requested by the Proposer to be treated as an Urgent Proposal; and

(b) has not been requested by the Proposer to be submitted directly to the Panel (or where it has been requested by the Proposer to be submitted directly to the Panel, the Panel has determined pursuant to Section D3.11 that the Draft Proposal should be referred to the Change Sub-Committee for further assessment).

D3.6 The Change Sub-Committee shall consider each Draft Proposal and the accompanying documents referred to in Section D3.4 at the next Change Sub-Committee meeting occurring more than 6 Working Days after the submission of the Draft Proposal.

D3.7 In considering each Draft Proposal, the Change Sub-Committee shall:

(a) provide views and comments to the Proposer on the scope of their Draft Proposal and any potential solution(s) put forward, and support the development of the Draft Proposal;

(b) if available, provide views and comments on any draft legal text submitted with the Draft Proposal;

(c) at its discretion, seek the views and input of the DCC and/or other Parties on the Draft Proposal; and

(d) make a recommendation to the Panel on whether the Draft Proposal should be progressed in parallel with any other Draft Proposals or Modification Proposals.

D3.8 At each meeting where it considers a Draft Proposal, the Change Sub-Committee shall determine whether the Draft Proposal:

(a) should remain with the Change Sub-Committee for further work and analysis, and if so what the timetable for this work shall be; or

(b) should be referred to the Panel for consideration on whether it should be progressed as a Modification Proposal, and if so recommend what the proposed progression timetable should be.

Initial Consideration by the Panel

D3.9 The Panel shall consider each Draft Proposal that:

(a) has been requested by the Proposer to be treated as an Urgent Proposal;

(b) has been requested by the Proposer to be submitted directly to the Panel; or

(c) has been referred to the Panel by the Change Sub-Committee following completion of its assessment.

D3.10 The Panel shall consider each Draft Proposal and the accompanying documents referred to in Section D3.4:

(a) in the case of Draft Proposals expressed by the Proposer to be urgent, within 5 Working Days after the proposal's submission; and

(b) in respect of all other Draft Proposals, at the next Panel meeting occurring more than 6 Working Days after the submission or referral (as applicable) of the Draft Proposal.

D3.11 In considering each Draft Proposal pursuant to Section D3.9, the Panel shall determine:

(a) whether to refuse the Draft Proposal in accordance with Section D3.14;

(b) whether the Draft Proposal should be referred to the Change Sub-Committee for further assessment; or

(c) whether the Draft Proposal should be progressed as a **Modification Proposal**.

D3.12 Where the Panel determines that a Draft Proposal should be progressed as a Modification Proposal, the Panel shall determine:

(a) not used;

(b) whether the Modification Proposal should be a Self-Governance Modification (taking into account the view expressed by the Proposer in the Draft Proposal and as described in Section D2), unless the Modification Proposal is an Authority-initiated Modification;

(c) whether the Authority should be asked to consider whether the Modification Proposal should be treated as an Urgent Proposal (and, where the Proposer has expressed the Modification Proposal to be urgent, the Panel shall so ask the Authority);

(d) in the case of Fast-Track Modifications, whether the Modification Proposal should be progressed and approved as a Fast-Track Modification (and such approval shall require the unanimous approval of all the Panel Members present at the relevant meeting, otherwise the Modification Proposal shall be progressed as though it is not a Fast-Track Modification);

(e) whether, in accordance with Section D3.15, it is necessary for the Modification Proposal to go through the Refinement Process, or whether it can progress straight to the Report Process;

(f) the timetable to apply in respect of the Modification Proposal, in accordance with the criteria set out in Section D3.16; and

(g) whether the Modification Proposal should be considered together with any other current Modification Proposal(s) (whether because they complement or contradict one another or for any other reason), in which case the Modification Proposals in question shall be considered by the same Working Group.

D3.13 The Secretariat shall, as soon as reasonably practicable following the Panel's determination under Sections D3.11 and D3.12 in respect of each Draft Proposal or Modification Proposal, confirm that determination to the Proposer and update the Modification Register.

Refusal by the Panel

D3.14 The Panel may not refuse an Authority-initiated Modification. Otherwise, the Panel may choose to refuse a Draft Proposal if that Draft Proposal has substantively the same effect as another Draft Proposal or Modification Proposal which was submitted by a Proposer on an earlier date and which:

(a) has not been refused, approved, rejected or withdrawn pursuant to this Section D at the time of the Panel's decision under this Section D3.14; or

(b) was refused or rejected pursuant to this Section D on a date falling within the period of two months immediately preceding the time of the Panel's decision under this Section D3.14.

Determining whether the Refinement Process should be followed

D3.15 The Panel shall determine whether each Modification Proposal must go through the Refinement Process, or whether it can progress straight to the Report Process. The Panel shall ensure that the following Modification Proposals are subject to the Refinement Process:

(a) those submitted by the Panel itself (other than Fast-Track Modifications);

(b) those that the Panel considers are likely to have an impact on the ability of the DCC to discharge its duties and comply with its obligations under the Relevant Instruments;

(c) those that the Panel considers are likely to require changes to DCC Systems, User Systems and/or Smart Metering Systems, and/or testing as part of implementation; or

(d) any other Modification Proposals, unless the Panel considers them to be clearly expressed and concerned solely with:

(i) insubstantial or trivial changes that are unlikely to be controversial (including typographical errors and incorrect cross-references); and/or

(ii) giving effect to variations that are mandated by the Relevant Instruments in circumstances where there is little or no discretion as to how they are to be given effect.

Timetable

D3.16 The Panel shall determine the timetable to be followed in respect of each Modification Proposal. In particular, the Panel shall:

(a) in the case of Authority-initiated Modifications, determine a timetable consistent with any relevant timetable issued by the Authority or the Secretary of State (as the case may be);

(b) in the case of Urgent Proposals, determine a timetable that is (or amend the existing timetable so that it becomes) consistent with any relevant timetable issued by the Authority; and

(c) (subject to Sections D3.16(a) and (b)) specify the date by which the Modification Report is to be finalised; being as soon as reasonably practicable after the Panel's decision in respect of such timetable (having regard to the complexity, importance and urgency of the Modification Proposal).

D3.17 The Panel may, whether at its own initiation or on the application of another person, determine amendments to the timetable applying from time to time to each Modification Proposal; provided that any such amendment is consistent with Section D3.16. The Secretariat shall, as soon as reasonably practicable following any Panel determination under this Section D3.17, confirm that determination to the Proposer and the Change Board and update the Modification Register.

D3.18 The Panel, the Code Administrator, the Secretariat, any relevant Working Group, the Change Board and the Parties shall each (insofar as within its reasonable control) complete any and all of the respective tasks assigned to them in respect of a Modification Proposal in accordance with the timetable applying to that Modification Proposal from time to time (including as provided for in Section D4.9).

D3.19 In determining or amending a timetable under Sections D3.10 and D3.11, the Panel may specify a time period for delivery of a DCC Assessment that differs from the standard time period set out in Section D6.10B (Analysis by the DCC). Without limitation, the Panel may specify a different time period in respect of Urgent DCC Assessments.

D4. AUTHORITY DETERMINATIONS

Authority Determination of Modification Path

D4.1 This Section D4.1 applies in respect of each Modification Proposal that the Panel has determined to be an Authority Determined Modification or a Self-Governance Modification. The Authority may:

(a) at its own initiation, or on the application of a Party or Citizens Advice or Citizens Advice Scotland; and

(b) having consulted with the Panel,

determine that the Modification Proposal should properly (in accordance with Section D2) be considered (in the case of an Authority Determined Modification) to be a Self- Governance Modification or be considered (in the case of a Self-Governance Modification) to be a Path 2 Modification. Any such determination shall be final and binding for the purposes of this Code.

Referral of Disputes to the Authority

D4.2 Where the Panel:

(a) refuses a Draft Proposal pursuant to Section D3 (Initial Assessment of Draft Proposals);

(b) determines that the Modification Proposal is an Authority-initiated Modification, an Authority Determined Modification or a Self-Governance Modification where such determination differs from the view of the Proposer expressed in the Draft Proposal; and/or

(c) determines a timetable (or an amendment to the timetable) in respect of the Modification Proposal which the Proposer considers inconsistent with the requirements of Section D3 (Initial Assessment of Draft Proposals),

then the Proposer may refer the matter to the Authority for determination in accordance with Section D4.3.

D4.3 The Proposer may only refer a matter to the Authority pursuant to Section D4.2 where such referral is made within 10 Working Days of the Proposer being notified by the Secretariat of the relevant matter. The Proposer shall send to the Panel a copy of any referral made pursuant to this Section D4.3.

D4.4 Where the Authority, after having consulted with the Panel, considers that the Panel's decision that is the subject of a matter referred to the Authority by a Proposer in accordance with Section D4.3 was made otherwise than in accordance with Section D3, then the Authority may determine the matter. Any such determination shall be final and binding for the purposes of this Code.

Authority Determination in respect of Urgent Proposals

D4.5 Where a Proposer has expressed a Draft Proposal to be urgent and/or where the Panel considers a Modification Proposal to be urgent, the Panel shall ask the Authority whether the Modification Proposal should be treated as an Urgent Proposal.

D4.6 A Modification Proposal shall only be an **Urgent Proposal** where the Authority directs the Panel to treat the Modification Proposal as an Urgent Proposal (whether following a referral by the Panel pursuant to Section D4.5, or at the Authority's own initiation).

D4.7 An Urgent Proposal shall be progressed:

(a) in accordance with any timetable specified by the Authority from time to time, and the Panel shall not be entitled to vary such timetable without the Authority's approval; and

(b) subject to any deviations from the procedure set out in this Section D as the Authority may direct (having consulted with the Panel).

Authority Determination in respect of Significant Code Reviews

D4.8 During a Significant Code Review Phase:

(a) the Panel shall report to the Authority on whether or not the Panel considers that any Draft Proposal or Modification Proposal on which the Change Board had not voted prior to the commencement of the Significant Code Review (whether submitted before or after the commencement of the Significant Code Review) falls within the scope of the Significant Code Review;

(b) the Panel may (subject to Section D4.8(d)) suspend the progress of any Draft Proposal or Modification Proposal that the Panel considers to fall within the scope of that Significant Code Review;

(c) the Authority may (subject to Section D4.8(d)) direct the Panel to suspend the progress of any Draft Proposal or Modification Proposal that the Authority considers to fall within the scope of that Significant Code Review (and the Panel shall comply with such directions); and

(d) the Authority may direct the Panel to cease the suspension of any Draft Proposal or Modification Proposal that has been suspended pursuant to this Section D4.8 (and the Panel shall comply with such directions). Any and all suspensions pursuant to this Section D4.8 shall automatically cease at the end of the Significant Code Review Phase.

D4.9 The commencement and cessation of suspensions in respect of a Modification Proposal pursuant to Section D4.8 shall have the effect of modifying the timetable applying to that Modification Proposal.

D5. WITHDRAWAL OF A PROPOSAL

Right to Withdraw

D5.1 Subject to Section D5.2, the Proposer for a Draft Proposal or a Modification Proposal may withdraw the Draft Proposal or Modification Proposal on notice to the Secretariat at any time prior to the decision of the Change Board under Section D8.14(b) in respect of that Draft Proposal or Modification Proposal.

D5.2 In the case of Authority-initiated Modifications, the Proposer may only withdraw the Draft Proposal or the Modification Proposal where the Proposer provides evidence that the Authority or the Secretary of State (as the case may be) has given its consent to such withdrawal. The Proposer may not withdraw a Modification Proposal following any direction by the Authority to the Panel pursuant to Section D9.3 (Send-Back Process).

D5.3 As soon as is reasonably practicable after receiving any notice in accordance with Section D5.1, the Secretariat shall notify the Parties that the Proposer has withdrawn its support and shall update the Modification Register accordingly.

Adoption of Withdrawn Proposals

D5.4 Where, within 10 Working Days of the Secretariat sending notice under Section D5.3, the Secretariat receives notice from a Party that it is prepared to adopt the Draft Proposal or the Modification Proposal, such Party shall (for all purposes in respect of this Code) be deemed thereafter to be the Proposer for the Draft Proposal or the Modification Proposal (and, where the Secretariat receives more than one such notice, the first such notice shall have priority over the others).

D5.5 Where Section D5.4 applies, the Draft Proposal or the Modification Proposal shall not be withdrawn, and the Secretariat shall notify the Parties and update the Modification Register.

Withdrawn Proposals

D5.6 Subject to Section D5.5, a Draft Proposal or a Modification Proposal that has been withdrawn in accordance with Section D5.1 shall cease to be subject to the process set out in this Section D.

Authority-initiated Modifications: Backstop Direction

D5.7 Where one or more Draft Proposals or Modification Proposals that are Authority initiated Modifications have been raised, the Authority or the Secretary of State (as the case may be) may issue a direction under this Section D5.7 that requires the withdrawal of those Draft Proposal or Modification Proposals, including any connected Alternative Solutions. Where the Authority or the Secretary of State (as the case may be) so directs:

(a) the Proposer for each such Modification Proposal shall be deemed to have withdrawn the Draft Proposal(s) or Modification Proposal(s), and Sections D5.3 and D5.4 shall not apply to the withdrawn Draft Proposal(s) or Modification Proposal(s); and

(b) where the direction is issued by the Authority, the Significant Code Review Phase shall re-commence.

D6. REFINEMENT PROCESS

Application of this Section

D6.1 This Section D6 sets out the **Refinement Process**. This Section D6 only applies in respect of a Modification Proposal where it is determined that the Modification Proposal is to be subject to the Refinement Process in accordance with Section D3 (Initial Consideration of Modification Proposals). The Refinement Process never applies to Fast-Track Modifications.

Establishment of a Working Group

D6.2 Where this Section D6 applies, the Panel shall establish a group of persons (a **Working Group**) for the purposes set out in Section D6.8. Such Working Groups shall be formed and operate in accordance with terms of reference as agreed by the Panel and published on the Website (the "Working Group Terms of Reference"). The Panel shall consult with Parties before it first establishes the Working Group Terms of Reference, and before it makes any changes to the Working Group Terms of Reference.

D6.3 Not used.

D6.4 Not used.

D6.5 Not used.

D6.6 Not used.

D6.7 Except to the extent inconsistent with this Section D6, the provisions of Section C6 (Sub-Committees) shall apply in respect of each Working Group as if that Working Group was a Sub-Committee.

Purpose of Refinement Process

D6.8 The purpose of the Refinement Process is to:

(a) consider and (to the extent necessary) clarify the likely effects of the Modification Proposal, including to identify the Parties, Party Categories, Energy Consumers and other persons likely to be affected by the Modification Proposal;

(b) evaluate and (to the extent necessary) develop and refine the content of the Modification Proposal;

(c) evaluate and (to the extent necessary) amend the proposed implementation timetable of the Modification Proposal including (where relevant) so as to ensure consistency with the SEC Release Management Policy (provided that the proposed implementation timetable of an Authority-initiated Modification cannot be so amended);

(d) consider (to the extent the Working Group considers necessary) the impact which the Modification Proposal would have, if approved, on the matters referred to in Section D6.9;

(e) consider whether the DCC should, as part of the proposal's implementation (if the Modification Proposal is approved), be required to undertake testing of the DCC Total System and/or provide testing services; and (if so) ensure that the Modification Proposal includes amendments to this Code which provide a robust testing solution (or, if it is not yet reasonably practicable to document the testing solution, which provide a process for developing the testing solution);

(f) seek (to the extent the Working Group considers necessary) the Technical Architecture and Business Architecture Sub-Committee’s views of the impact which the Modification Proposal would have, if approved, on the DCC Systems and Smart Metering Systems; provided that the Working Group shall always seek such views:

  (i) in respect of proposals to modify the Technical Code Specifications; and/or

  (ii) where the Technical Architecture and Business Architecture Sub- Committee has notified the Working Group that the Technical Architecture and Business Architecture Sub-Committee wishes to express a view;

(g) seek (to the extent the Working Group considers necessary) the Security Sub- Committee's views on the Modification Proposal; provided that the Working Group shall always seek such views:

  (i) in respect of proposals to modify the Security Obligations and Assurance Arrangements; and/or

  (ii) where the Security Sub-Committee has notified the Working Group that the Security Sub-Committee wishes to express a view;

(h) seek (to the extent the Working Group considers necessary) the SMKI PMA’s views on the Modification Proposal; provided that the Working Group shall always seek such views:

  (i) in respect of proposals to modify the SMKI SEC Documents; and/or

  (ii) where the SMKI PMA has notified the Working Group that the SMKI PMA wishes to express a view;

(i) seek (to the extent the Working Group considers necessary) the Alt HAN Forum's views on the Modification Proposal; provided that the Working Group shall always seek such views:

  (i) in respect of proposals to modify Section Z (The Alt HAN Arrangements);

  (ii) in respect of proposals to modify any SEC Subsidiary Document which relates to Section Z (The Alt HAN Arrangements);

  (iii) in respect of proposals to modify Section K (Charging Methodology) which are likely to affect the Alt HAN Charges; and/or

  (iv) where the Alt HAN Forum (or a Forum Sub-Group acting on its behalf) has notified the Working Group that it wishes to express a view;

(j) consider whether, if the Modification Proposal is approved, this Code would better facilitate the achievement of the SEC Objectives than if the Modification Proposal was rejected;

(k) consider whether it is likely that there would be a material impact on Greenhouse Gas Emissions as a result of the Modification Proposal being approved, and (if so) assessing such impact (which assessment shall be conducted in accordance with any guidance on the evaluation of Greenhouse Gas Emissions issued by the Authority from time to time); and

(l) consider whether, if the Modification Proposal is approved, changes are likely to be required to other Energy Codes as a result.

Analysis by the DCC

D6.9 In considering the matters referred to in Section D6.8(d) and (e), each Working Group for a Modification Proposal shall consider whether one or more DCC Assessments should be undertaken in respect of the Modification Proposal. At the request from time to time of a Working Group for a Modification Proposal, the DCC shall prepare a DCC Preliminary Assessment and/or a DCC Impact Assessment for one or more (in whole or in part) of the following areas for analysis, as determined by the Working Group:

(a) whether the DCC should, as part of the proposal's implementation (if that Modification Proposal were to be approved), be required to undertake testing of the DCC Total System and/or provide testing services; and (if so) the DCC's proposals for the scope, phases, timetable and participants for such testing (or, to the extent it is not yet reasonably practicable to determine such matters, its proposals for the process pursuant to which such matters should be developed);

(b) how the ability of the DCC to discharge its duties and comply with its obligations under the Relevant Instruments would be affected if that Modification Proposal were to be approved; and/or

(c) the extent to which changes would be required to DCC Systems if the Modification Proposal were to be approved; and/or

(d) the DCC's best estimate of the likely implementation and operating costs associated with the changes that would be required to DCC Systems if the Modification Proposal were to be approved, and any consequential impact on the Charges.

D6.10 Within 5 Working Days (unless otherwise agreed with the Working Group) after receiving notice from the Working Group of the requirement for a DCC Assessment, the DCC shall confirm if there is any additional information it reasonably needs (and shall provide a description of such required additional information) to complete the DCC Assessment or shall otherwise confirm that the request for a DCC Assessment has been accepted. The Code Administrator, within 5 Working Days (unless otherwise agreed with the Working Group), shall provide any information so requested (where it has such information), or shall otherwise co-ordinate efforts to obtain such information from the Working Group

D6.10A Where additional information is requested in accordance with Section D6.10 or this D6.10A, the DCC shall, within 5 Working Days after receiving such additional information, confirm if there is still more additional information it reasonably needs (and provide a description of such required additional information) to complete the DCC Assessment or shall otherwise confirm that the request for a DCC Assessment has been accepted.

D6.10B The DCC shall complete each DCC Assessment and present it to the Code Administrator within 15 Working Days (for DCC Preliminary Assessments) or 40 Working Days (for DCC Impact Assessments) measured in each case from acceptance by the DCC under Section D6.10 or D6.10A; subject to amendments to the timetable made by the Panel under Section D3.11 (Timetable) or agreed by the relevant Working Group in accordance with Section D6.10C.

D6.10C Where the DCC considers at any time that it will not be able to complete a DCC Assessment within the time period required by Section D6.10B, the DCC may apply to the relevant Working Group to request an amendment to the DCC Assessment timescales. The DCC shall provide the Working Group with reasons in respect of any such request, and shall propose a revised timescale for delivery with an explanation of how it is to be achieved. Any such amendment proposed by the DCC shall only be effective if agreed by the Working Group. The Working Group may not agree an amendment which would require a deviation from the then current timetable applying to the Modification Proposal under Sections D3.10 and D3.11 (Timetable).

D6.10D Where the DCC wishes to amend a DCC Assessment timescale which requires a deviation from the then current timetable applying to the Modification Proposal under Sections D3.10 and D3.11 (Timetable) or where the relevant Working Group does not agree to an amendment under Section D6.10C, then the DCC may apply to the Panel to request an amendment to the DCC Assessment timescale in accordance with Section D3.11 (Timetable). The DCC shall give reasons in respect of any such request, which must also be notified to the Working Group so that members of the Working Group can also make submissions to the Panel if they wish to do so.

D6.10E Prior to requesting a DCC Impact Assessment, the Working Group shall refer the Modification Proposal to the Change Board for it to determine whether a DCC Impact Assessment should be requested. The Working Group shall not request a DCC Impact Assessment unless the Change Board has determined, following a vote as referred to in Section D8.14A, that it shall be requested.

D6.11 In considering whether the approval of a Modification Proposal would better facilitate the achievement of the SEC Objectives than the rejection of the Modification Proposal, the Working Group shall have regard to any and all DCC Assessments provided by the DCC.

Working Group Consultation

D6.12 Each Working Group established pursuant to this Section D6 in respect of a Modification Proposal shall consider any representations made to it by Parties from time to time regarding the subject-matter of the Modification Proposal.

D6.13 Each Working Group established pursuant to this Section D6 in respect of a Modification Proposal shall undertake at least one formal consultation in respect of the Modification Proposal seeking views on the matters set out in Section D6.8. The Working Group shall consult with the Parties, Citizens Advice or Citizens Advice Scotland and (where appropriate) any interested third parties (including, where relevant, Energy Consumers and/or those who represent or advise Energy Consumers).

D6.14 Each Working Group established pursuant to this Section D6 in respect of a Modification Proposal shall publish on the Website, and bring to the Parties' attention, a document (the **Consultation Summary**) containing the following:

(a) the final consultation draft of the Modification Proposal, including in particular the legal text of the proposed variation and the proposed implementation timetable;

(b) all consultation responses received and not marked as confidential; and

(c) a statement of whether the Working Group considers that the approval of the Modification Proposal would better facilitate the achievement of the SEC Objectives than the rejection of the Modification Proposal (and if so why).

Alternative Solutions

D6.15 The Proposer shall have full ownership of the Proposed Solution to a Modification Proposal, and may direct changes to this variation at any time during the Refinement Process as long as any revised solution continues to achieve the purpose of the Modification Proposal.

D6.16 The Working Group may raise one or more Alternative Solution(s) where the majority of the Working Group considers that there is more than one variation to this Code that could achieve the purpose of the Modification Proposal (and that each such variation would, if made, better facilitate the achievement of the SEC Objectives than if that variation were not made),

D6.17 References in this Section D to a Modification Proposal shall (except where the context otherwise requires) be deemed to include reference to the Proposed Solution and any Alternative Solution(s) raised in accordance with Section D6.16.

D7. REPORT PHASE

Modification Report

D7.1 The Code Administrator shall, in respect of each Modification Proposal, prepare a written report on the proposal (the **Modification Report**); provided that no Modification Report shall be required for Fast-Track Modifications. This stage of the process is referred to as the **Report Phase**.

D7.2 The Code Administrator shall prepare the Modification Report for each Modification Proposal:

(a) where the Refinement Process has been followed, in accordance with the instructions of the relevant Working Group; or

(b) where the Refinement Process has not been followed, on the basis of the Modification Proposal and in consultation with the Proposer.

Content of the Modification Report

D7.3 The Modification Report for each Modification Proposal shall:

(a) be addressed and delivered to the Panel;

(b) set out the legal text of the proposed variation to this Code (and, where applicable, set out the alternative legal text of the Alternative Proposal);

(c) specify the proposed implementation timetable (including the proposed implementation date);

(d) specify the likely effects of the proposed variation if it is implemented;

(e) specify, in the opinion of the Working Group (or, where the Refinement Process was not followed, the Code Administrator), which Party Categories are likely to be affected by the Modification Proposal;

(f) specify whether, if the Modification Proposal is approved, this Code would better facilitate the achievement of the SEC Objectives than if the Modification Proposal was rejected;

(g) specify whether it is likely that there would be a material impact on Greenhouse Gas Emissions as a result of the Modification Proposal being approved, and (if so) assessing such impact (which assessment shall be conducted in accordance with any guidance on the evaluation of Greenhouse Gas Emissions issued by the Authority from time to time);

(h) specify whether, if the Modification Proposal is approved, changes are likely to be necessary to other Energy Codes, and whether changes have been proposed in respect of the affected Energy Codes; and

(i) where the Modification Proposal was subject to the Refinement Process prior to the Report Phase:

(i) include the Consultation Summary produced by the Working Group in respect of the Modification Proposal;

(ii) specify whether, if the Modification Proposal is approved, the implementation of the Modification Proposal is likely to require changes to DCC Systems, User Systems and/or Smart Metering Systems; and (if so) the likely development, capital and operating costs associated with such changes and any consequential impact on the Charges;

(iii) specify whether, if the Modification Proposal is approved, the DCC is to be required, as part of the Modification Proposal's implementation, to undertake testing of the DCC Total System and/or provide testing services; and (if so) how such testing is dealt with in the Modification Proposal;

(iv) include a summary of any views provided by the Technical Architecture and Business Architecture Sub-Committee, the Security Sub- Committee, the SMKI PMA or the Alt HAN Forum in respect of the Modification Proposal pursuant to Section D6.8 (Purpose of the Refinement Process); and

(v) include a summary and copies of any and all DCC Assessments provided by the DCC pursuant to Section D6.9 (Analysis by the DCC).

Consideration of the Modification Report

D7.4 Upon completion of the Modification Report, the Code Administrator will place such report on the agenda for the next meeting of the Panel. Where the Refinement Process was followed, a member of the relevant Working Group shall attend that Panel meeting, and may be invited to present the findings of the Working Group to the Panel and/or answer the questions of Panel Members in respect of the Modification Report.

D7.5 The Panel shall consider each Modification Report and shall determine whether to:

(a) return the Modification Report back to the Working Group (or, where there was no Refinement Process, the Code Administrator) for further clarification or analysis (in which case, the Panel shall determine the timetable and terms of reference of such further analysis); or

(b) allow the Modification Report to proceed to the Modification Report Consultation.

D7.6 The Panel shall not make any statement regarding whether it believes the Modification Proposal should be successful.

D7.7 Where the Panel determines that a Modification Report is to proceed to the Modification Report Consultation, the Panel shall determine:

(a) the timetable for such Modification Report Consultation, including the period for which the consultation is to remain open (which cannot be more than 15 Working Days); and

(b) the Party Categories that the Panel considers are likely to be affected by the Modification Proposal.

Modification Report Consultation

D7.8 Where the Panel determines that a Modification Report is to proceed to the Modification Report Consultation, the Code Administrator shall arrange for a consultation seeking the views of Parties (other than the DCC) on the Modification Report (the **Modification Report Consultation**). The Code Administrator shall:

(a) invite consultation responses in accordance with the timetable determined by the Panel and in the form referred to in Section D7.9;

(b) collate the responses received during the consultation, and add those responses to the Modification Register; and

(c) place the Modification Report on the agenda for the next meeting of the Change Board following the collation of such consultation responses.

D7.9 Each Modification Report Consultation shall allow for each Party (other than the DCC) that wishes to respond to the consultation to respond by way of a form that provides for a response in one of the following manners (where applicable, in respect of the Proposed Solution Proposal and the Alternative Solution(s) separately):

(a) 'no interest' where the Party considers that it and its Party Category are unlikely to be affected by the Modification Proposal;

(b) 'abstain' where the Party wishes to abstain for reasons other than as described in Section D7.9(a);

(c) 'approve' where the Party considers that making the variation would better facilitate the achievement of the SEC Objectives than if the variation was rejected; or

(d) 'reject' where the Party considers that not making the variation would better facilitate the achievement of the SEC Objectives than if the variation was approved,

(e) and which prompts the Party to give a reason for its response by reference to the SEC Objectives.

D7.10 Each Party's response to a Modification Report Consultation will only be validly given if made on the forms provided and received on or before the deadline for responses.

D8. CHANGE BOARD AND CHANGE BOARD DECISION

Establishment of the Change Board

D8.1 The Panel shall establish a Sub-Committee as described in this Section D8, to be known as the **Change Board.** Save as expressly set out in this Section D8, the Change Board shall be subject to the provisions concerning Sub-Committees set out in Section C6 (Sub-Committees).

Function of the Change Board

D8.2 The function of the Change Board shall be to:

(a) decide whether a Modification Proposal is ready for a DCC Impact Assessment to be requested;

(b) consider each Modification Report and the responses received in response to the Modification Report Consultation;

(c) decide whether to approve or reject the Modification Proposal in the form set out in the Modification Report (and, where there is at least one Alternative Solution, confirm whether the approval or rejection relates to the Proposed Solution or to an Alternative Solution); and

(d) decide whether to approve or reject a proposed Authority-Led Variation.

Effect of the Change Board Decision

D8.3 The effect of the Change Board decision shall:

(a) in the case of Authority-initiated Modifications, Authority-Determined Modifications and Authority-Led Variations, be to recommend to the Authority that the variation be approved or rejected; or

(b) in the case of Self-Governance Modifications, be to approve or reject the variation.

Membership of the Change Board

D8.4 The following persons shall serve on the Change Board (each being a **Change Board Member):**

(a) one person nominated jointly by Citizens Advice and Citizens Advice Scotland;

(b) one person appointed by each of the Voting Groups within the Party Category representing the Large Supplier Parties;

(c) three persons appointed by the Party Category representing the Small Supplier Parties;

(d) three persons appointed by the Party Categories representing Electricity Network Parties and the Gas Network Parties collectively; and

(e) three persons appointed by the Party Category representing the Other SEC Parties.

D8.5 Each Voting Group, Party Category or Party Categories (as applicable) referred to in each sub-section of Section D8.4 shall nominate its appointee(s) to serve as Change Board Member(s) to the Secretariat. Each Change Board Member shall serve for a term of one year, and shall be capable of being reappointed at the end of that term. The relevant Voting Group, Party Category or Party Categories may (on notice to the Secretariat) establish a rota whereby more than one person shares the office of Change Board Member.

D8.6 It shall be for the Parties within the relevant Party Category or Party Categories (as applicable) referred to in each sub-section of Section D8.4 to determine how they agree between themselves on the identity of each person to be appointed as a Change Board Member on their behalf. In the event that the Parties within such Party Category or Party Categories cannot so agree, the Secretariat shall seek the preference of the Parties within the relevant Party Category or Party Categories (as applicable) and the person preferred by the majority of those Parties that express a preference (on a one-vote-per- Party basis) shall be appointed as a Change Board Member. In the absence of a majority preference the relevant Change Board Member position shall remain unfilled.

D8.7 The Panel shall only be entitled to remove a Change Board Member from office where such Change Board Member is repeatedly absent from meetings to an extent that frustrates the proceedings of the

Change Board. The Voting Group by which a Change Board Member was appointed pursuant to Section D8.4(b) shall be entitled to remove that Change Board Member by notice in writing to the Secretariat. The Party Category or Party Categories (as applicable) referred to in each other sub-section of Section D8.4 shall be entitled to remove the Change Board Member appointed by them from office by notice in writing to the Secretariat; provided that the majority of the Parties within the relevant Party Category or Party Categories (as applicable) must approve such removal.

Duties of Change Board Members

D8.8 The Consumer Member serving on the Change Board will, when acting as a Change Board Member, act in a manner consistent with the statutory functions of Citizens Advice or Citizens Advice Scotland. Each other Change Board Member will act in the interests of the Voting Group, Party Category or Party Categories (as applicable) by which the Change Board Member was appointed.

D8.9 In giving effect to his or her duties under Section D8.8, each Change Board Member (other than the Consumer Member) shall:

(a) be guided (but not bound) by the responses to the Modification Report Consultation given by Parties within the Voting Group, Party Category, or Party Categories (as applicable) by which such Change Board Member was appointed;

(b) seek to clarify with the relevant Party any responses to the Modification Report Consultation that are not clear to the Change Board Member, or which the Change Board Member considers to be based on a misunderstanding of the facts;

(c) seek to act in the best interests of the majority, whilst representing the minority view (and, where a majority is not significant, the Change Board Member should consider whether abstention from the vote best represents the interests of the Change Board Member's constituents); and

(d) be entitled to vote or abstain without regard to the Panel's indication of which Party Categories the Panel considered to be affected by the Modification Proposal.

D8.10 The confirmation to be given by each Change Board Member to SECCo in accordance with Section C6.9 (Member Confirmation) shall refer to Section D8.8 in place of Section C6.8.

Proceedings of the Change Board

D8.11 The Code Administrator shall chair the Change Board meetings. The chair shall have no vote (casting or otherwise).

D8.12 The quorum for Change Board meetings shall be:

(a) at least three persons appointed by the Large Supplier Parties;

(b) at least one person appointed by the Small Supplier Parties;

(c) at least two persons appointed by the Electricity Network Parties and Gas Network Parties collectively; and

(d) at least one person appointed by the Other SEC Parties,

(e) provided that fewer (or no) appointees from a Party Category shall be required where that Party Category has not appointed that many (or any) Change Board Members; and further provided that no appointees from a Party Category shall be required where the Panel indicated pursuant to Section D7.7(b) that that Party Category was not likely to be affected by the Modification Proposal in question.

D8.13 In addition to those persons referred to in Section C5.13, representatives of the DCC shall be entitled to attend and speak (but not vote) at each meeting of the Change Board.

The Change Board Vote

D8.14 In respect of each Modification Report referred to the Change Board, the Change Board shall vote:

(a) whether to determine that the Modification Report should be returned to the Working Group (or, where there was no Refinement Process, the Code Administrator) for further clarification or analysis; and if not

(b) whether to approve the Proposed Solution or any Alternative Solution set out in the Modification Report (on the basis that the Change Board may only approve one of them).

D8.14A In respect of each request for a DCC Impact Assessment submitted by a Working Group pursuant to Section D6.10E, the Change Board shall vote on whether to request the DCC Impact Assessment or whether to return the Modification Proposal to the Working Group for further work.

D8.15 A vote referred to in Sections D8.14 or D8.14A shall take the form of a vote by:

(a) the Consumer Member serving on the Change Board;

(b) the Change Board Members appointed by the Voting Groups within the Party Category representing the Large Supplier Parties (whose collective vote shall be determined in accordance Section D8.16);

(c) the Change Board Members appointed by the Party Category representing the Small Supplier Parties (whose collective vote shall be determined in accordance with Section D8.16);

(d) the Change Board Members appointed by the Party Categories representing Electricity Network Parties and the Gas Network Parties (collectively) (whose collective vote shall be determined in accordance with Section D8.16); and

(e) the Change Board Members appointed by the Party Category representing the Other SEC Parties (whose collective vote shall be determined in accordance with Section D8.16),

(f) and a vote pursuant to Sections D8.14 or D8.14A shall only be successfully passed if the majority of the votes cast in accordance with this Section D8.15 are cast in favour. For the avoidance of doubt: an abstention shall be treated as if no vote was cast; where there are no Change Board Members present from within the categories referred to in each of Sections D8.15(a) to (e) they shall be deemed to have abstained; and a tie amongst the votes cast shall not be a vote in favour.

D8.16 Each of the collective votes by Change Board Members referred to in Section D8.15(b) to (e) shall be determined by a vote among the relevant Change Board Members, such vote to be undertaken on the basis:

(a) of one vote per Change Board Member; and

(b) that the majority of those Change Board Members that are present must vote in favour in order for the collective vote to be considered a vote in favour (and, for the avoidance of doubt, a tie amongst the votes cast shall not be a vote in favour).

D8.17 In casting his or her vote, each Change Board Member must record the reason for his or her vote, and where voting on whether or not to approve a variation must explain whether the making of the variation would better facilitate the achievement of the SEC Objectives than if the variation was rejected.

Communicating the Change Board Vote

D8.18 Following the vote of the Change Board in respect of each Modification Report, the Code Administrator shall update the Modification Register to include the outcome of the vote and the reasons given by the Change Board Members pursuant to Section D8.17.

D8.19 Where the outcome of the Change Board vote is to determine that the Modification Report should be returned for further clarification or analysis (as referred to in Section D8.14(a)), the Working Group (or, where there was no Refinement Process, the Code Administrator) shall update the Modification Report to include such clarification or analysis, and this shall be returned to the Panel at the next suitable meeting.

D8.20 Where the Change Board votes on whether to approve a variation set out in a Modification Report (as referred to in Section D8.14(b)), the Code Administrator shall communicate the outcome of that vote to the Authority and the Panel, and shall send copies of the following to the Authority:

(a) the Modification Report;

(b) the Modification Report Consultation and the responses received in respect of the same; and

(c) the outcome of the Change Board vote, including the reasons given by the Change Board Members pursuant to Section D8.17.

D8.21 Where the outcome of the Change Board vote referred to in Section D8.14A is a decision that a DCC Impact Assessment should not be requested, the Change Board shall specify the further work it believes is required in order for it to reconsider whether a DCC Impact Assessment should be requested. The Proposer may appeal the decision to the Panel. Where, following an appeal made to it, the Panel determines that a DCC Impact Assessment is not to be requested, the Panel shall specify the further work it believes is required in order for the Change Board to reconsider whether a DCC Impact Assessment should be requested. Once this further work has been completed, the Working Group may re-refer the Modification Proposal to the Change Board to determine whether a DCC Impact Assessment should be requested.

D9. MODIFICATION PROPOSAL DECISION

General

D9.1 The final decision as to whether or not to approve a Modification Proposal shall depend upon whether the Modification Proposal is:

(a) an Authority-initiated Modification or an Authority Determined Modification;

(b) a Self-Governance Modification; or

(c) a Fast-Track Modification.

Authority-initiated Modifications and Authority Determined Modifications

D9.2 An Authority-initiated Modification or an Authority Determined Modification shall only be approved where the Authority determines that the Modification Proposal shall be approved (which determination shall, without prejudice to section 173 of the Energy Act 2004, be final and binding for the purposes of this Code). In making such determination, the Authority will have regard to:

(a) its objectives and statutory duties under the Electricity Act and the Gas Act;

(b) whether or not the approval of the variation would better facilitate the achievement of the SEC Objectives than if the variation was rejected;

(c) the decision of the Change Board in respect of the Modification Proposal, which shall be considered to constitute a recommendation by the Parties as to whether or not to approve the Modification Proposal; and

(d) such other matters as the Authority considers appropriate.

Send-Back Process

D9.3 Where the Authority considers that it is unable to form an opinion in relation to a Modification Proposal submitted to it, then it may issue a direction to the Panel specifying any additional steps that the Authority requires in order to form such an opinion (including drafting or amending the proposed legal text, revising the proposed implementation timetable, and/or revising or providing additional analysis and/or information). Where the Authority issues a direction to the Panel pursuant to this Section D9.3:

(a) the decision of the Change Board in respect of the Modification Proposal shall be null and void;

(b) the Panel shall send the Modification Proposal back to the relevant Working Group (or shall establish a Working Group) to consider the matters raised by the Authority, and to prepare a revised Modification Report;

(c) the Panel shall revise the timetable applying to the Modification Proposal; and

(d) the Secretariat shall update the Modification Register to record the status of the Modification Proposal.

Self-Governance Modifications

D9.4 A Self-Governance Modification shall only be approved where the Change Board votes to approve the Modification Proposal, subject to the following:

(a) any Party that disagrees with the decision of the Change Board, may (within 10 Working Days following the publication of that decision) refer the matter to the Panel, and the Panel shall determine whether it wishes to reverse the decision of the Change Board;

(b) any Party that disagrees with the decision of the Panel pursuant to Section D9.4(a), may (within 10 Working Days following the publication of that decision) refer the matter to the Authority, and the Authority shall determine whether the Modification Proposal should be rejected or approved in accordance with Section D9.2 (which determination shall, without prejudice to section 173 of the Energy Act 2004, be final and binding for the purposes of this Code); and

(c) accordingly, where the consequence of the Panel's or the Authority's determination is that the Modification Proposal is to be rejected (where it has previously been approved) the Modification Proposal shall be cancelled and not implemented (or, if already implemented, shall be reversed).

Fast-Track Modifications

D9.5 In the case of a Fast-Track Modification, any decision of the Panel under Section D3.6 to approve the Modification Proposal shall be final, subject to the following:

(a) any Party that disagrees with the Modification proposal being approved as a Fast-Track Modification, may (within 15 Working Days following the publication of that decision) object to the decision; and

(b) where an objection is received, the Panel's decision on the Modification proposal shall be cancelled and the Modification proposal shall be returned to the Panel at its next meeting. The Panel shall then revise its determination under Section D3.6 as though the Modification Proposal is not a Fast-Track Modification.

D9A AUTHORITY-LED VARIATIONS

Authority Power to Develop a Proposed Variation

D9A.1 The Authority may develop a proposed variation to this Code in respect of a Significant Code Review, in accordance with the procedures set out in this Section D9A.

D9A.2 The Authority may commence a Significant Code Review Phase by issuing a direction under this Section D9A.2, or may issue a direction under this Section D9A.2 at any time during a Significant Code Review Phase. The Authority's direction under this Section D9A.2 will set out the scope and/or subject matter of the Significant Code Review.

Authority-Led Consultation

D9A.3 The Authority will, in such manner as it considers appropriate, consult on the merits of the proposed Authority-Led Variation with the Parties, Citizens Advice, Citizens Advice Scotland, and any other persons whose interests are materially affected by this Code.

Authority-Led Modification Report

D9A.4 The Authority may submit its proposed Authority-Led Variation to the Code Administrator, together with such supplemental information as the Authority considers appropriate.

D9A.5 Upon receipt of the Authority's proposal under Section D9A.4, the Code Administrator shall prepare a written report on the proposal (the "Authority-Led Modification Report"). The Authority-Led Modification Report must be consistent with the information provided by the Authority under Section 9A.4, and shall:

(a) be addressed and delivered to the Panel;

(b) set out the legal text of the proposed variation to this Code;

(c) specify the proposed implementation timetable (including the proposed implementation date);

(d) specify the likely effects of the proposed variation if it is implemented;

(e) specify which Party Categories are likely to be affected by the proposed variation;

(f) specify whether the implementation of the proposed variation will require changes to DCC Systems, User Systems and/or Smart Metering Systems; and (if so) the likely development, capital and operating costs associated with such changes and any consequential impact on the Charges;

(g) specify whether, if the proposed variation is approved, this Code would better facilitate the achievement of the SEC Objectives than if the proposed variation was rejected;

(h) specify whether it is likely that there would be a material impact on Greenhouse Gas Emissions as a result of the proposed variation being approved, and (if so) assessing such impact (which assessment shall be conducted in accordance with any guidance on the evaluation of Greenhouse Gas Emissions issued by the Authority from time to time); and

(i) specify whether, if the proposed variation is approved, changes are likely to be necessary to other Energy Codes, and whether changes have been proposed in respect of the affected Energy Codes.

D9A.6 Upon completion of the Authority-Led Modification Report, the Code Administrator will place such report on the agenda for the next meeting of the Panel, which shall refer the report to the Change Board.

Change Board and Change Board Decision

D9A.7 In respect of each Authority-Led Modification Report referred to the Change Board, the Change Board shall vote whether to approve the Authority-Led Variation.

D9A.8 Each vote as referred to in Section D9A.7 shall take the form of a vote in accordance with Sections D8.15 to D8.17 (The Change Board Vote). The Authority's Significant Code Review conclusions document and/or the Authority's proposal submitted in accordance with Section D9A.4 shall not fetter the procedures or voting rights referred to in Section D8 (Change Board and Change Board Decision).

D9A.9 Following the vote of the Change Board in respect of the Authority-Led Variation, the Code Administrator shall populate the Modification Register to include the outcome of the vote and the reasons given by the Change Board Members pursuant to Section D8.17 (The Change Board Vote).

D9A.10 The Code Administrator shall communicate the outcome of the Change Board vote to the Authority and the Panel, and shall send copies of the following to the Authority:

(j) the Authority-Led Modification Report; and

(k) the outcome of the Change Board vote, including the reasons given by the Change Board Members pursuant to Section D8.17 (The Change Board Vote).

Authority Decision

D9A.11 An Authority-Led Variation shall be approved only where the Authority determines that the proposed variation shall be approved (which determination shall, without prejudice to section 173 of the Energy Act 2004, be final and binding for the purposes of this Code). In making such determination, the Authority will have regard to:

(l) its objectives and statutory duties under the Electricity Act and the Gas Act;

(m) whether or not the approval of the variation would better facilitate the achievement of the SEC Objectives than if the variation was rejected;

(n) the decision of the Change Board in respect of the variation, which shall be considered to constitute a recommendation by the Parties as to whether or not to approve the variation; and

(o) such other matters as the Authority considers appropriate.

Send-Back Process

D9A.12 Where the Authority considers that it is unable to form an opinion in relation to a proposed Authority-Led Variation, then it may issue a direction to the Panel specifying any additional steps that the Authority requires in order to form such an opinion. Where the Authority issues a direction to the Panel pursuant to this Section D9A.12:

(p) the decision of the Change Board in respect of the variation shall be null and void;

(q) the Panel shall seek to address the matters raised by the Authority, and shall (where necessary) have an updated Authority-Led Modification Report produced; and

(r) the Secretariat shall update the Modification Register to record the status of the proposed variation.

Implementation

D9A.13 Where an Authority-Led Variation has been approved in accordance with Section D9A.11, Section D10 (Implementation) shall apply.

D10. IMPLEMENTATION

General

D10.1 Once a Modification Proposal has been approved in accordance with Section D9 (Modification Proposal Decision) or an Authority-Led Variations has been approved in accordance with Section D9A.11 (Authority Decision), the Panel shall ensure that this Code is varied in accordance with the Modification Proposal or Authority-Led Variation, as set out in this Section D10. Authority-Led Variations are to be treated as Authority-initiated Modifications for the purposes of this Section D10 (and references to Modification Proposals shall be interpreted accordingly).

Implementation

D10.2 The Panel shall, at the next Panel meeting after a Modification Proposal has been approved:

(a) determine what actions are required in order to ensure that the approved variation to this Code is made in accordance with the approved implementation timetable; and

(b) set a timetable for the completion of each of those actions.

D10.3 It shall be the duty of the Panel to ensure that the actions which are required to secure that an approved variation to this Code is made in accordance with the approved implementation timetable are taken.

D10.4 Each Party shall co-operate with the Panel to the extent required to ensure that such variation is made with effect from such date.

Subsequent Amendment to Implementation Timetable

D10.5 Where, having regard to representations received from the Code Administrator or from any Party, the Panel considers that it is not reasonably practicable to make the approved variation to this Code in accordance with the approved implementation timetable:

(a) the Panel may request the Authority to direct that a new implementation timetable be substituted for the first such timetable; and

(b) where the Authority makes such a direction following a request by the Panel, the implementation timetable directed by the Authority shall have effect in substitution for the first such timetable, and the requirements of this Section D10 shall be defined by relation to that later date.

D10.6 Without prejudice to the generality of Section D10.5, the Panel shall make a request to the Authority under that Section where:

(a) the decision of the Authority to approve the relevant Modification Proposal is subject to an appeal pursuant to section 173 of the Energy Act 2004 or is challenged by judicial review; and

(b) the Panel considers that it is appropriate in the circumstances for the timetable to be delayed given such appeal or challenge.

SEC Release Management Policy

D10.7 The implementation of an approved Modification Proposal will take place as part of a SEC Release. The Panel shall ensure that the implementation of a SEC Release is undertaken in accordance with a policy for determined by the Panel (the "Panel SEC Release Management Policy").

D10.8 The Panel shall ensure that the SEC Release Management Policy:

(a) includes a mechanism for allocating Modification Proposals into SEC Releases;

(b) defines a mechanism by which the Panel shall co-ordinate and oversee the content; and

(c) defines a mechanism by which notice is to be given to Users prior to the implementation of a SEC Release;

(d) defines a mechanism by which the Panel shall review the main components of the forecast and actual costs of a SEC release and, if requested by the Authority, how the Panel, shall provide a report on this to the Authority; and

(e) defines a mechanism by which the Panel shall determine that the SEC Release shall be put into live operation.

D10.9 The Panel shall make the Panel Release Management Policy available to the DCC and Users on the SEC Website. The Panel shall consult with the DCC and Users before it first establishes the Panel Release Management Policy, and before it makes any changes to the Panel Release Management Policy.

D10.10 The DCC shall co-operate with the Panel in planning and implementing SEC Releases in accordance with the SEC Release Management Policy and shall provide any information reasonably requested by the Panel for this purpose.

D10.11 The Panel may appoint, or require DCC to appoint, an external auditor to monitor the DCC's implementation process, plans and progress in support of a SEC Release, and shall approve any such external auditor's terms of reference. The DCC must co-operate with any external auditor that is appointed, including (but not limited to) allowing access to such records, test results, test laboratories and test witnessing as the external auditor may reasonably require.

SEC Release Implementation Document

D10.12 The Panel shall develop and publish a "SEC Release Implementation Document" for each SEC Release in accordance with the SEC Release Management Policy.

D10.13 The Panel shall ensure that each SEC Release Implementation Document:

(a) defines the content of the SEC Release;

(b) defines the timescales associated with implementing the content of the SEC Release, including timescales for the commencement and completion of DCC and User testing phases;

(c) defines how the DCC shall report progress towards readiness;

(d) defines the testing that will be undertaken by the DCC for the SEC Release;

(e) defines the required User testing and how the DCC shall support Users to test the changes that make up the SEC Release; and

(f) defines the SEC Release go-live criteria that shall be agreed by the Panel in accordance with the SEC Release Management Policy.

D10.14 The DCC shall provide any information reasonably requested by the Panel that is required for inclusion in the SEC Release Implementation Document for a SEC Release.

D10.15 The Panel shall approve the SEC Release Implementation Document and any subsequent amendments.

D10.16 The DCC shall be required to undertake the implementation and testing activities for a SEC Release as set out in the relevant SEC Release Implementation Document once approved by the Panel.

D10.17 Any Party that wishes to appeal the Panel approval of the SEC Release Implementation Document may do so within 10 Working Days following the publication of the decision to approve. Any appeal referred to the Authority, must specify the reasons for the appeal. The Authority shall determine what action to take with the appeal (which determination shall, without prejudice to section 173 of the Energy Act 2004, be final and binding for the purposes of this Code).

SEC Release Testing Approach Document

D10.18 The DCC, on request of the Panel, shall produce a document setting out how the requirements of Sections D10.13(d) and (e) will be satisfied (the "SEC Release Testing Approach Document"). A SEC

Release Testing Approach Document shall be considered as part of the SEC Release Implementation Document for the relevant SEC Release.

D10.19 The DCC shall ensure that each SEC Release Testing Approach Document sets out the following, as a minimum, in respect of the SEC Release in question:

(a) the proposed amendments to this Code that are the subject of the testing, an explanation of the associated changes to the DCC Total System, and the testing objective;

(b) the testing environments and test phases to be used and how these will be sequenced;

(c) the Devices to be used in testing (including the use of emulators);

(d) the requirements (if any) for security testing;

(e) the requirements (if any) for system capacity testing;

(f) details of the testing that shall be undertaken, including the scope of testing and the extent of testing (including negative tests) and the approach to regression testing and End Of Cycle testing;

(g) the applicable Testing Issue thresholds and the process by which DCC may propose to exclude Testing Issues from being counted against the Testing Issue thresholds;

(h) the process and expected timescales for managing the resolution of extant Testing Issues following completion of a test phase;

(i) the entry criteria that must be met in order for a test phase to commence and who approves entry;

(j) the exit criteria that must be met in order for a test phase to complete and who approves exit;

(k) any key risks (and risk mitigation) identified in respect of the proposed approach to testing;

(l) the approach to providing assurance of the testing undertaken;

(m) matters to be included in DCC's test completion reports presented to the Panel; and

(n) the requirements (if any) for User testing and for determining any associated test completion.

D10.20 The DCC shall prepare and consult upon each SEC Release Testing Approach Document and any subsequent amendments. The DCC shall report to the Panel on the outcome of each such consultation. The Panel shall review and determine whether to approve each SEC Release Testing Approach Document and any subsequent amendments.

D10.21 The DCC and each person other than the DCC that participates in (or is required to participate in) testing under a SEC Release Testing Approach Document shall comply with the document approved by the Panel (including such amendments as are approved by the Panel from time to time).

Programme Assurance Policy

D10.22 The Panel shall establish and maintain a policy (the "**Programme Assurance Policy**") to govern DCC-initiated projects and programmes that have the potential to impact Users but which do not require a Modification.

D10.23 In the case where the DCC implements a project or programme that has the potential to impact Users (but which does not require a Modification), the DCC shall adhere to the Programme Assurance Policy. For clarity, this may include DCC Internal System Changes.

D10.24 The DCC shall plan and implement DCC projects and programmes in accordance with the Programme Assurance Policy, and shall co-operate with the Panel and provide any and all information reasonably requested by the Panel for this purpose.

D10.25 In developing the Programme Assurance Policy, and prior to making any subsequent change to it, the Panel shall consult with the DCC and have regard to the views of all Parties.

D10.26 The Panel shall ensure that an up-to-date copy of the Programme Assurance Policy is made available to all Parties and is published on the Website.

D10.27 In developing or making changes to the Programme Assurance Policy, the Panel shall ensure that it gives due consideration to the need for the DCC to: (a) comply at all times with the 'General Objectives of the Licensee' (as defined in the DCC Licence); and (b) efficiently discharge the other obligations imposed upon the DCC by the DCC Licence.

D10.28 Should the DCC disagree with the Panel on any changes made to the Programme Assurance Policy (in accordance with the provisions of this Section D10), the DCC may refer the matter to the Authority for determination, whose decision shall be final and binding for the purposes of this Code.

D11. DCC ASSESSMENT REPORTING

Reporting on DCC Assessments

D11.1 The DCC shall report to the Panel each month on the status of all DCC Assessments which are ongoing or that have been completed since the last such report. The DCC shall include in each such report any additional details reasonably requested by the Panel since the last such report.

D11.2 Such reports shall include details of whether the required timescales for completion of the DCC Assessments are likely to be (or have been) met. Where there is any delay, the DCC shall set out a clear explanation of the reasons for such delay, the likely delivery timescales, and the actions being taken by the DCC to minimise the delay.

Code Performance Measures

D11.3 Each of the following performance measures constitute a Code Performance Measure (to which the following Target Service Level and Minimum Service Level will apply, measured over the following Performance Measurement Period):

No.	Code Performance Measure	Performance Measurement Period	Target Service Level	Minimum Service Level
9	Out of the DCC Assessments required to be completed during the Performance Measurement Period, how	Monthly	100%	100%

	many were completed within the required timescales.			

D12. LEAD CODE AND CONSEQUENTIAL CHANGES

Cross Code Steering Group

D12.1 The Panel shall from time to time nominate to the REC Code Manager one or more individuals to represent the Panel on the Cross Code Steering Group. The Panel shall ensure that each of the nominated individuals has the appropriate skills, knowledge and experience to participate in accordance with the Cross Code Steering Group's terms of reference.

D12.2 The Panel may discharge the requirements of Section D12.1 by ensuring the Code Administrator provides appropriate representatives.

Lead Code

D12.3 Where the Cross Code Steering Group determines that this Code is to be used as the Lead Code, the Code Administrator shall:

(a) progress the Lead Code Modification in accordance with this Code;

(b) coordinate with the other affected Energy Codes so that they can progress a Consequential Change under their Energy Code in parallel with the process under this Code;

(c) publish a timetable setting out the proposed progression of the Lead Code Modification and any associated Consequential Changes; and

(d) notwithstanding Section D9 (Modification Proposal Decision), the Modification Proposal under this Code shall only be approved if both:

(i) the Modification Proposal is approved in accordance with this Code; and

(ii) the associated Consequential Changes under the other Energy Codes are all approved in accordance with those other Energy Codes.

Consequential Change

D12.4 Where the Cross Code Steering Group determines that another Energy Code is the Lead Code for a Modification Proposal, then the Code Administrator shall progress the relevant Consequential Change to this Code in accordance with this Section D, but subject to the following:

(a) the Code Administrator shall progress the Modification to the timetable determined under the Lead Code;

(b) if the Lead Code Modification under the Lead Code is withdrawn or rejected prior to a Change Board determination the Code Administrator shall Withdraw the Consequential Change in accordance with Section D5 except that Sections D5.4 and D5.5 shall not apply.

(c) notwithstanding Section D9 (Modification Proposal Decision), the Modification Proposal under this Code shall only be approved if both:

(i) the Modification Proposal is approved in accordance with this Code; and

(ii) the variation to the Lead Code is approved in accordance with the Lead Code.

Appeal to the Authority

D12.5 The Panel may appeal the determination of any associated Consequential Change to the Authority where:

(a) this Code is the Lead Code;

(b) the Lead Code Modification is approved;

(c) one or more associated Consequential Changes are not approved; and

(d) such an appeal is raised within 30 Working Days of a determination on the Lead Code Modification or relevant Consequential Change.

D12.6 Where another Energy Code is the Lead Code any determination under this Code on an associated Consequential Change may be sent to the Authority for appeal within 30 Working Days of such a determination on request of the Lead Code (in which case the approval or rejection of the Consequential Change shall be determined by the Authority as if Section D9.2 applied).

Energy Market Data

D12.7 Where a Modification Proposal is progressed in relation to an Energy Market Message and/or an Energy Market Data Item defined within the Energy Market Data Specification, the relevant Energy Market Meta Data Owner shall be defined as the Lead Code.

D12.8 The Code Administrator shall ensure that the meta data for all relevant Energy Market Messages and Energy Market Data Items utilised under this Code are defined within the Energy Market Data Specification administered in accordance with the REC Change Management Schedule.

E REGISTRATION DATA

E1. RELIANCE ON REGISTRATION DATA

DCC

E1.1 The DCC shall, from time to time, use and rely upon the Data previously provided to it by RDPs or provided by the CSS Provider pursuant to Section E2 as most recently updated pursuant to Section E2 (**Registration Data**) or pursuant to Section E5 (the **Additional Registration Data**); provided that the DCC shall be allowed up to three hours from receipt to upload such Data to the DCC Systems.

E1.2 Without prejudice to the generality of Section E1.1, the DCC shall use and rely upon the Registration Data and, where applicable, the Additional Registration Data when:

(a) assessing a User's eligibility to receive certain Services (as described in Section H4 (Processing Service Requests); and

(b) calculating the Charges payable by a Party.

E1.3 The DCC shall have no liability to any Party where it provides (or does not provide) a Service in circumstances where it should not (or should) have done so, to the extent that the same arises due to inaccuracies in the Registration Data or the Additional Registration Data that are not caused by the DCC.

Panel

E1.4 The Panel shall periodically request from the DCC any Registration Data and Additional Registration Data reasonably required by the Panel in relation to the proper exercise of its duties, powers and functions, including the Registration Data required by the Panel to establish into which Party Category a Party falls. Where aggregated or anonymised data (or similar) is sufficient for the Panel's needs, the Panel shall request, and the DCC shall provide, the data in such format.

E1.5 The DCC shall provide to the Panel any Registration Data and Additional Registration Data requested by the Panel in accordance with Section E1.4.

E1.6 The Panel (and the Secretariat) shall, from time to time, use and rely upon the Registration Data and the Additional Registration Data most recently provided to the Panel pursuant to Section E1.5.

E2. PROVISION OF DATA

Responsibility for Providing Electricity and Gas Registration Data

E2.1 The CSS Provider shall provide to the DCC electricity Registration Data as required under the REC.

E2.2 The CSS Provider shall provide to the DCC gas Registration Data as required under the REC.

Obligation on DCC to Provide Data to RDPs

E2.3 The DCC shall provide the information set out in Section E2.4 to the Registration Data Provider nominated by each Electricity Network Party and each Gas Network Party (as such information is further described in the Registration Data Interface Documents).

E2.4 The information to be provided by the DCC:

(a) to each Electricity Network Party's Registration Data Provider is:

(i) whether there is an Enrolled Smart Metering System associated with each of the MPANs relating to the Electricity Network Party's network (and the date of its Enrolment); and

(ii) the identity of the person which the DCC believes to be Registered in respect of each of the MPANs relating to the Electricity Network Party's network; and

(b) to each Gas Network Party's Registration Data Provider is whether there is an Enrolled Smart Metering System associated with each of the Supply Meter Points on the Gas Network Party's network (and the date of its Enrolment).

Frequency of Data Exchanges

E2.5 The Data to be provided by the DCC to the RDPs under this Section E2 shall be provided by way of incremental updates to Data previously provided (so that only Data that has changed is updated).

E2.6 The incremental updates to Data to be provided in accordance with this Section E2 shall be made at the frequency and/or time required in accordance with the Registration Data Interface Documents.

E2.7 The Data to be provided by the CSS Provider under this Section E2 shall be sent as per the requirements for provisions of such data as specified in the REC.

Registration Data Interface

E2.8 The DCC shall maintain the Registration Data Interface in accordance with the Registration Data Interface Specification, and make the interface available to the Registration Data Providers to receive Data via the DCC Gateway Connections in accordance with the Registration Data Interface Code of Connection.

E2.9 The DCC shall ensure that the Registration Data Interface is available at all times (subject to Planned Maintenance undertaken in accordance with Section H8.3).

E2.10 Each Electricity Network Party and each Gas Network Party shall ensure that its Registration Data Provider shall (when acting in such capacity) comply with the applicable obligations set out in the Registration Data Interface Documents and the Incident Management Policy.

E2.11 For the avoidance of doubt, the DCC shall comply with the applicable obligations set out in the Registration Data Interface Documents and the Incident Management Policy (as it is obliged to do in respect of all applicable provisions of this Code).

E2.12 Not used

E2.13 Where the DCC identifies any omissions or manifest errors in the Registration Data, the DCC shall seek to resolve any such omissions or manifest errors in accordance with the Incident Management Policy. In such circumstances, the DCC may continue (notwithstanding Section E1.1) to rely upon and use any or all of the Registration Data that existed prior to its receipt of the incremental update that included any such omission or manifest error, unless the Incident Management Policy provides for an alternative course of action.

RDP Security Obligations

E2.14 Each Electricity Network Party and each Gas Network Party shall ensure that its Registration Data Provider (being the Network Party itself where that is deemed to be the case in accordance with the definition of Registration Data Provider) shall (when acting in its capacity as the Network Party's Registration Data Provider) comply with the obligations expressed to be placed on Users and identified in Section E2.15 as if, in the case of each such obligation:

(a) references to User were references to such Registration Data Provider; and

(b) references to User Systems were references to the RDP Systems of that Registration Data Provider.

E2.15 The obligations identified in this Section E2.15 are those obligations set out at:

(a) Sections G3.2 to G3.3 (Unauthorised Activities: Duties to Detect and Respond);

(b) Sections G3.8 to G3.9 (Management of Vulnerabilities);

(c) Sections G5.14 to G5.18 (Information Security: Obligations on Users), save that for this purpose the reference:

(i) in Section G5.18(b)(i) to "Sections G3 and G4" shall be read as if it were to "Sections G3.2 to G3.3 and G3.8 to G3.9"; and

(ii) in Section G5.18(b)(iii) to "Sections G5.19 to G5.24" shall be read as if it were to "Section G5.19(d)".

E2.16 Each Electricity Network Party and each Gas Network Party shall ensure that its Registration Data Provider (being the Network Party itself where that is deemed to be the case in accordance with the definition of Registration Data Provider) shall (when acting in its capacity as the Network Party's Registration Data Provider) propose to the DCC one or more EUI-64 Compliant identification numbers, issued to the RDP by the Panel, to be used by that RDP when acting in its capacity as such (save that it may use the same identification number when acting as an RDP for more than one Network Party).

E2.17 The DCC shall accept each identification number proposed by each Registration Data Provider for the purposes set out in Section E2.16 (and record such numbers as identifying, and use such numbers to identify, such RDP when acting as such); provided that the DCC shall only accept the proposed number if it has been issued by the Panel.

Security Obligations on CSS Provider

E2.18 The CSS Provider shall comply with the obligations expressed to be placed on Users and identified in Section E2.15 as if, in the case of each such obligation:

(a) references to User were references to the CSS Provider; and

(b) references to User Systems were references to the CSS Provider Systems.

E2.19 The CSS Provider shall ensure that any Registration Data that it sends is Digitally Signed using a Private Key that is associated with a Public Key contained within an Organisation Certificate.

E2.20 The DCC shall only use Registration Data received from the CSS Provider if:

(a) it has successfully carried out a Check Cryptographic Protection in respect of that Registration Data and successfully carried out a Confirm Validity of the Organisation Certificate used to Check Cryptographic Protection; and

(b) the DCC has not previously successfully carried out the checks set out in paragraph E2.20(a) on that Registration Data.

Disputes

E2.21 Any Dispute regarding compliance with this Section E2 may be referred to the Panel for its determination, which shall be final and binding for the purposes of this Code; save that Disputes regarding compliance with Section E2.14 shall be subject to the means of Dispute resolution applying to the provisions of Section G (Security) referred to in Section E2.15 (as set out in Section G).

Provision of Further Data

E2.22 The Parties agree that the DCC may send the notification in Section E2.23 and the associated information set out in Section E2.24 to the CSS Provider.

E2.23 The notification referred to in Section E2.22 is a notification that a Smart Meter has been added to the Device Log of a Communications Hub.

E2.24 The information referred to in Section E2.22 is any information held in the Smart Metering Inventory that pertains to either the Communications Hub referred to in Section E2.23 or to any Smart Meter that is listed in the Device Log of that Communications Hub.

E3. DCC GATEWAY CONNECTIONS FOR REGISTRATION DATA PROVIDERS

Provision of a DCC Gateway Connection for RDPs

E3.1 Registration Data Providers may request DCC Gateway Connections, and the DCC shall offer to provide such connections, in accordance with Sections H15.4 and H15.6 to H15.12 (as if Registration Data Providers were Parties), save that a Registration Data Provider shall not specify which DCC Gateway Bandwidth Option it requires, and shall instead specify which (if any) other Registration Data Providers it intends to share the connection with pursuant to Section E3.4.

E3.2 The DCC shall provide DCC Gateway Connections to the premises of Registration Data Providers in accordance with Sections H15.13 to H15.15 (as if Registration Data Providers were Parties), save that no Charges shall apply.

E3.3 The DCC shall ensure that the DCC Gateway Connection it provides to the premises of Registration Data Providers pursuant to this Section E3 is of a sufficient bandwidth to meet the purposes for which such connection will be used by the Registration Data Provider, and any other Registration Data Providers notified to the DCC in accordance with Section E3.1 or E3.4 (provided, in the case of those notified in accordance with Section E3.4, that the DCC may object to the transfer or sharing where it reasonably believes that the connection will not be of sufficient bandwidth to meet the needs of all of the Registration Data Providers in question).

E3.4 Each Registration Data Provider may transfer or share its rights in respect of the DCC Gateway Connection provided to its premises pursuant to this Section E3 in accordance with Sections H15.16 and H15.17 (as if Registration Data Providers were Parties), save that such rights may only be transferred to or shared with other Registration Data Providers for the purposes of accessing the Registration Data Interface.

E3.5 Once a DCC Gateway Connection has been established:

(a) the Registration Data Provider that requested it (or to whom it has been transferred in accordance with Section E3.4) and the DCC shall each comply with the provisions of the DCC Gateway Connection Code of Connection applicable to the DCC Gateway Bandwidth Option utilised at the connection; and

(b) the DCC shall make the connection available to such Registration Data Provider until: (i) the DCC is notified by such Registration Data Provider that it wishes to cancel the connection; or (ii) such Registration Data Provider ceases to be a Registration Data Provider for one or more Network Parties.

DCC Gateway Equipment at RDP Premises

E3.6 The DCC and each Registration Data Provider shall comply with the provisions of Sections H15.20 to H15.28 in respect of the DCC Gateway Equipment installed (or to be installed) at a Registration Data Provider's premises (as if Registration Data Providers were Parties), save that Section H15.28 shall be construed by reference to Section E3.5(b).

Interpretation

E3.7 Given the application of certain provisions of Section H15 to Registration Data Providers in accordance with this Section E3, defined terms used in Section H15 and/or the DCC Gateway Connection Code of Connection shall be construed accordingly (including DCC Gateway Party by reference to the Registration Data Provider which requested the connection, or to whom the right to use the connection has been transferred pursuant to Sections E3.4 and H15.16). Given that Registration Data Providers do not specify the DCC Gateway Bandwidth Option that they require (and that the DCC instead determines the most appropriate bandwidth), references in Section H15 to the bandwidth requested by a Party shall be construed accordingly.

Liability of and to the Network Parties

E3.8 Each Network Party shall ensure that its Registration Data Provider (being the Network Party itself where that is deemed to be the case in accordance with the definition of Registration Data Provider) shall comply with the obligations expressed to be placed on Registration Data Providers under or pursuant to this Section E3.

E3.9 Where more than one Network Party nominates the same Registration Data Provider, each of those Network Parties shall be jointly and severally liable for any failure by that Registration Data Provider to comply with the obligations expressed to be placed on Registration Data Providers under or pursuant to this Section E3.

E3.10 The DCC acknowledges that it is foreseeable that Network Parties will have made arrangements with their Registration Data Providers such that breach by the DCC of this Section E3 will cause the Network Parties to suffer loss for which the DCC may be liable (subject to Section M2 (Limitations of Liability)).

Disputes

E3.11 Where a Registration Data Provider wishes to raise a dispute in relation to its request for a DCC Gateway Connection, then the dispute may be referred to the Panel for determination. Where that Registration Data Provider or the DCC disagrees with any such determination, then it may refer the matter to the Authority for its determination, which shall be final and binding for the purposes of this Code.

E4. RDP ENTRY PROCESS

Overview

E4.1 Before Data is exchanged between the DCC and a Registration Data Provider under Section E2 (Provision of Data) for the first time, the Registration Data Provider must successfully complete the RDP Entry Process Tests.

RDP Entry Process Tests

E4.2 The "**RDP Entry Process Tests**" are, in respect of an RDP, tests to demonstrate that the DCC and the RDP are capable of exchanging Data under Section E2 (Provision of Data), as such tests are further described in the Enduring Testing Approach Document. An RDP which successfully completed Code Implementation SIT shall be deemed to have successfully completed the RDP Entry Process Tests.

E4.3 Each RDP that has not (and is not deemed to have) successfully completed the RDP Entry Process Tests shall be entitled to undertake RDP Entry Process Tests. Each RDP that has been nominated by one or more Network Parties for which the RDP was not nominated at the time that it successfully completed the RDP Entry Process Tests (or was deemed to do so) shall be entitled to undertake RDP Entry Process Tests in relation to such Network Parties. Each RDP is only obliged to successfully complete the RDP Entry Process Tests once.

E4.4 Each RDP that undertakes RDP Entry Process Tests shall:

(a) do so in accordance with Section H14 (Testing Services) and the Enduring Testing Approach Document; and

(b) be a Testing Participant for the purposes of RDP Entry Process Tests (and the provisions of Section H14 shall apply accordingly, including in respect of Testing Issues).

E4.5 The RDP will have successfully completed the RDP Entry Process Tests once the DCC considers that both it and the RDP have demonstrated that they have satisfied the applicable requirements set out in the Enduring Testing Approach Document.

E4.6 Where requested by the RDP, the DCC shall provide written confirmation to the RDP confirming whether or not the DCC considers that the RDP Entry Process Tests have been successfully completed.

E4.7 Where the DCC is not satisfied that the RDP Entry Process Tests have been successfully completed, the RDP may refer the matter to the Panel for its determination. Where the RDP disagrees with any such determination of the Panel, then the RDP may refer the matter to the Authority for its determination (which shall be final and binding for the purposes of this Code).

Liability of and to the Network Parties

E4.8 Each Network Party shall ensure that its Registration Data Provider (being the Network Party itself where that is deemed to be the case in accordance with the definition of Registration Data Provider) shall comply with the obligations expressed to be placed on Registration Data Providers under or pursuant to this Section E4. An RDP need not enter into an Enabling Services Agreement (and Section H14.7 shall not apply to RDPs).

E4.9 Where more than one Network Party nominates the same Registration Data Provider, each of those Network Parties shall be jointly and severally liable for any failure by that Registration Data Provider to comply with the obligations expressed to be placed on Registration Data Providers under or pursuant to this Section E4.

E4.10 The DCC acknowledges that it is foreseeable that Network Parties will have made arrangements with their Registration Data Providers such that breach by the DCC of this Section E4 will cause the Network Parties to suffer loss for which the DCC may be liable (subject to Section M2 (Limitations of Liability)).

E5. ADDITIONAL REGISTRATION DATA

Electricity Data

E5.1 Each Electricity Network Party shall with effect from calendar month October 2020 provide (or procure that its Registration Data Provider provides) to the DCC by no later than the last day of each calendar month (the '**relevant calendar month**') the data referred to in Section E5.2 in respect of each Electricity Supplier Party.

E5.2 The data to be provided to the DCC by the Electricity Network Party in accordance with Section E5.1 is the number of Metering Points on its network that relate to Designated Premises at which:

(a) the Electricity Supplier Party is Registered on the 15th day of the relevant calendar month; and

(b) the quantity of electricity supplied to the premises is measured by an Electricity Meter that is an Advanced Meter,

(**Electricity Additional Registration Data**).

Gas Data

E5.3 Each Gas Network Party shall with effect from calendar month October 2020 provide (or procure that its Registration Data Provider provides) to the DCC by no later than the last day of each calendar month (the '**relevant calendar month**') the data referred to in Section E5.4 in respect of each Gas Supplier Party.

E5.4 The data to be provided to the DCC by the Gas Network Party in accordance with Section E5.3 is the number of Supply Meter Points on its network that relate to Designated Premises at which:

(a) the Gas Supplier Party is Registered on the 15th day of the relevant calendar month; and

(b) the quantity of gas supplied to the premises is measured by a Gas Meter that is an Advanced Meter, (Gas Additional Registration Data).

Contents

F SMART METERING SYSTEM REQUIREMENTS

F1. TECHNICAL SUB-COMMITTEE

Establishment of the Technical Sub-Committee

F1.1 The Panel shall establish a Sub-Committee in accordance with the requirements of this Section F1, to be known as the "**Technical Architecture and Business Architecture Sub-Committee**".

F1.2 Save as expressly set out in this Section F1, the Technical Architecture and Business Architecture Sub-Committee shall be subject to the provisions concerning Sub- Committees set out in Section C6 (Sub-Committees).

F1.3 Membership of the Technical Architecture and Business Architecture Sub-Committee shall be determined by the Panel:

(a) having regard to the need to provide an appropriate level of technical and business architecture expertise in the matters that are the subject of the Technical Architecture and Business Architecture Sub-Committee's duties; and

(b) otherwise in accordance with Section C6.7 (Membership).

Duties of the Technical Architecture and Business Architecture Sub-Committee

F1.4 The Technical Architecture and Business Architecture Sub-Committee shall undertake the following duties on behalf of the Panel:

(a) to provide the Panel, the Change Sub-Committee, the Change Board and Working Groups with technical and business architecture support and advice in respect of Draft Proposals and Modification Proposals that provide for variations to the Technical Code Specifications (or variations to other parts of this Code that affect the End-to-End Technical Architecture and/or the Business Architecture);

(b) to provide the Panel, the Change Sub-Committee, the Change Board and Working Groups with technical and business architecture support and advice in respect of Draft Proposals and Modification Proposals that are identified as likely (if approved) to require changes to the End-to-End Technical Architecture and/or to the Business Architecture;

(c) to provide the Authority (on request) with such information as the Authority may request regarding the technical aspects of any Notification (or potential Notification);

(d) to provide the Panel with technical and business architecture support and advice in respect of Disputes for which the Panel is required to make a determination, insofar as such Disputes relate to the Technical Code Specifications (or other parts of this Code that affect the End-to-End Technical Architecture and/or the Business Architecture);

(e) to review (where directed to do so by the Panel) the effectiveness of the End-to- End Technical Architecture (including so as to evaluate whether the Technical Code Specifications continue to meet the SEC Objectives), and report to the Panel on the outcome of such review (such report to include any recommendations for action that the Technical Architecture and Business Architecture Sub-Committee considers appropriate);

(f) to review (where directed to do so by the Panel) the effectiveness of the Business Architecture (including their assessment against the SEC Objectives), in consultation with Parties and Competent Authorities (but without engaging directly with Energy Consumers), and report to the Panel on the outcome of such review (such report to include any recommendations for action that the Technical Architecture and Business Architecture Sub-Committee considers appropriate);

(g) to review (where directed to do so by the Panel) the effectiveness of the HAN Requirements (including their assessment against the SEC Objectives), in consultation with Parties and Competent Authorities (but without engaging directly with Energy Consumers), and report to the Authority and the Panel on the outcome of such review;

(h) to support the Panel in the technical and business architecture aspects of the annual report which the Panel is required to prepare and publish under Section C2.3(h) (Panel Duties);

(i) to develop and thereafter maintain the Technical Architecture Document and the Business Architecture Document, and arrange for their publication on the Website;

(j) to provide the Panel with support and advice in respect of any other matter (not expressly referred to in this Section F1.4) which is concerned with the End-to- End Technical Architecture and/or the Business Architecture;

(k) (to the extent to which it reasonably considers that it is necessary to do so) to liaise and exchange information with, provide advice to, and seek the advice of the Alt HAN Forum on matters that relate to the End-to-End Technical Architecture and/or the Business Architecture; and

(l) to perform any other duties expressly ascribed to the Technical Architecture and Business Architecture Sub-Committee elsewhere in this Code.

F1.5 In undertaking its duties under Section F1.4(e) to (g), the Technical Architecture and Business Architecture Sub-Committee shall not review the Alt HAN Arrangements but may have regard to any impact of the provision of Alt HAN Services on the End-to- End Technical Architecture and/or the Business Architecture.

F1.6 The Technical Architecture and Business Architecture Sub-Committee shall establish a process whereby the Code Administrator monitors Draft Proposals and Modification Proposals with a view to identifying (and bringing to the Technical Architecture and Business Architecture Sub-Committee's attention) those proposals that are likely to affect the End-to-End Technical Architecture and/or the Business Architecture. The Code Administrator shall comply with such process.

F1.7 The Panel shall make each report produced pursuant to Section F1.4 available to the Parties, subject to any redactions it considers necessary to avoid a risk of Compromise to the DCC Total System, User Systems, RDP Systems and/or Devices.

DCC Obligations

F1.8 The DCC shall provide all reasonable assistance and information to the Technical Architecture and Business Architecture Sub-Committee in relation to the performance of its duties as it may reasonably request, including by providing the Technical Architecture and Business Architecture Sub-Committee with any requested Solution Architecture Information.

Provision of Information in respect of HAN Requirement Reviews

F1.9 Each Party shall provide to the Technical Architecture and Business Architecture Sub- Committee all such information as it may reasonably request in relation to its reviews of the HAN Requirements.

F2. CENTRAL PRODUCTS LIST

Central Products List

F2.1 The Panel shall establish and maintain a list (the "**Central Products List**") of:

(a) the SMETS2+ Device Models for which the Panel has received all the Assurance Certificates required for the Physical Device Type relevant to that Device Model (known as the Certified Products List); and

(b) in the case of SMETS1 Device Models, those Device Models for which the Panel has received all the information required in accordance with the CPL Requirements Document (which does not require any certification of SMETS1 Devices under the CPA or any other assurance scheme).

F2.2 The Panel shall ensure that the Central Products List identifies the Data required in accordance with the CPL Requirements Document, and that the Central Products List is updated to add and remove Device Models in accordance with the CPL Requirements Document (including as described in Section F2.7A).

F2.2A Where a Party disagrees with any decision of the Panel to add, remove, not remove, reinstate, or not reinstate a SMETS1 Device Model to or from the Central Products List, that Party may refer the matter to the Authority for its determination, which shall be final and binding for the purposes of this Code.

Background to Assurance Certificates

F2.2B For SMETS1 Device Models, there are no required Assurance Certificates for any of the Physical Device Types.

F2.3 The Technical Specification relevant to the Physical Device Type sets out which Physical Device Types require Assurance Certificates from one or more of the following persons (each being an "**Assurance Certification Body**"):

(a) the ZigBee Alliance;

(b) the DLMS User Association; and

(c) NCSC.

F2.4 The following Assurance Certification Bodies issue the following certificates in respect of Device Models of the relevant Physical Device Types (each being, as further described in the applicable Technical Specification, an "**Assurance Certificate**"):

(a) the ZigBee Alliance issues certificates which contain the ZigBee certified logo and interoperability icons;

(b) the DLMS User Association issues certificates which include the conformance tested service mark (" **DLMS Certificates**"); and

(c) NCSC issues commercial product assurance scheme certificates ("**CPA Certificates**").

F2.5 An Assurance Certificate will not be valid unless it expressly identifies the Device Model(s) and the relevant Physical Device Type to which it applies. With the exception of a CPA Certificate, an Assurance Certificate will not be valid if it specifies an expiry date that falls more than 6 years after its issue.

Expiry and renewal of CPA Certificates

F2.6 As CPA Certificates that have not been withdrawn or cancelled will require periodic renewal at their expiry or renewal date, the following Parties shall ensure that action is taken to ensure that a CPA Certificate can be considered for renewal in respect of Device Models for the following Physical Device Types before the expiry or renewal date of such CPA Certificate (to the extent Device Models of the relevant Physical Device Type require CPA Certificates in accordance with the applicable Technical Specification):

(a) the DCC for Communications Hubs; and

(b) the Import Supplier and/or Gas Supplier (as applicable) for Device Models of all other Physical Device Types.

F2.7 The Panel shall notify the Parties on or around the dates occurring 12 and 6 months prior to the date on which the CPA Certificate for any Device Model is due to expire. The Panel shall also provide to the Parties any notice concerning CPA Certificates which the NCSC asks the Panel to provide to the Parties.

Consequence of Expiry, Withdrawal or Cancellation of Assurance Certificates

F2.7A Where:

(a) a CPA Certificate for a Device Model expires or is not renewed or is withdrawn or cancelled by the NCSC, then the Security Sub-Committee shall determine whether to remove that Device Model from the Central Products List in accordance with the CPL Requirements Document, which may provide for a CPA Certificate Remedial Plan to be imposed;

(b) any other type of Assurance Certificate for a Device Model is withdrawn or cancelled by the Assurance Certification Body that issued the certificate, then the Panel shall remove that Device Model from the Central Products List.

F2.7B Where a Party disagrees with any decision of the Security Sub-Committee made in accordance with the CPL Requirements Document:

(a) to remove or not remove a Device Model from the Central Products List;

(b) to not approve the Party's CPA Certificate Remedial Plan (where the Security Sub-Committee has determined that a CPA Certificate Remedial Plan is to be imposed on the Party),

that Party may refer the matter to the Authority for its determination, which shall be final and binding for the purposes of this Code.

Publication and Use by the DCC

F2.8 Subject to the requirements of the CPL Requirements Document, the Panel shall (within one Working Day after being required to add or remove Device Models to or from the Central Products List in accordance with the CPL Requirements Document):

(a) provide the updated Central Products List to the DCC (by way of an extract containing such subset of the information contained within the Central Products List as the DCC reasonably requires from time to time);

(b) publish a copy of the updated Central Products List on the Website; and

(c) notify the Parties that the Central Products List has been updated.

F2.9 Subject to the requirements of the CPL Requirements Document, the DCC shall, from time to time, use and rely upon the Central Products List most recently received by the DCC from the Panel at that time, provided that the DCC shall be allowed up to 24 hours from receipt to make any modifications to the Smart Metering Inventory that are necessary to reflect the updated Central Products List.

Deployed Products List

F2.10 The DCC shall create, keep reasonably up-to-date and provide to the Panel (and the Panel shall publish on the Website) a list (the "**Deployed Products List**") of all the combinations of different Device Models that comprise a Smart Metering System (together with Associated Type 2 Devices) that exist from time to time (to the extent recorded by the Smart Metering Inventory).

SMETS1 Lists

F2.10A The DCC shall create, keep up-to-date and provide to the Panel (and the Panel shall publish on the Website) lists of:

(a) each combination of SMETS1 Device Models and communication services provider in relation to which the DCC has demonstrated through testing (which may include testing of a different combination that the DCC considers to be substantively equivalent) that it is able to successfully process SMETS1 Service Requests and relevant SMETS1 Alerts (the "**SMETS1 Eligible Product Combinations**"), including the date on which each entry was first added to the list; and

(b) each combination of SMETS1 Device Models and communication services provider) in relation to which the DCC is at that time:

(i) considering whether testing or development is required to demonstrate the capability; or

(ii) developing and/or testing the capability,

to successfully process SMETS1 Service Requests and relevant SMETS1 Alerts (the "**SMETS1 Pending Product Combinations**"), provided that the DCC shall not add a Device Model combination to the SMETS1 Pending Product Combinations where the relevant Testing Participant has indicated pursuant to clause 9 (SMETS1 Pending Product Combinations Tests) of the Enduring Testing Approach Document that such information should be treated as confidential.

F2.10B The obligation of the DCC under Section F2.10A(a) shall only apply once the DCC is first permitted under the Transition and Migration Approach Document to add a combination of Device Models to the SMETS1 Eligible Product Combinations.

Technical Specification Incompatibility

F2.11 The Panel shall create, keep reasonably up-to-date and publish on the Website a matrix specifying:

(a) which Versions of each Technical Specification are incompatible with which Versions of each other Technical Specification; and

(b) where applicable, those areas in respect of which the Version of the Technical Specification is not incompatible with the Version of the other Technical Specification but may be subject to the application of particular constraints as identified

F2.12 For the purposes of Section F2.11:

(a) 'incompatible' means in respect of a Version of any Technical Specification, that Devices or apparatus which comply with that Version are known to have been designed in a manner that does not enable them to inter-operate fully with Devices or apparatus that comply with the specified Version of each other Technical Specification;

(b) each reference to a Version of a Technical Specification shall be read as being to that Version taken together with any relevant Version of the GB Companion Specification (as identified in the TS Applicability Tables), so that if there is more than one relevant Version of the GB Companion Specification for any Version of a Technical Specification, the matrix shall make separate provision for each of them; and

(c) the matrix need not specify:

(i) which Versions of the ESMETS are incompatible with Versions of the GSMETS;

(ii) which Versions of the GSMETS are incompatible with which Versions of:

(A) the ESMETS;

(B) the HCALCSTS; or

(C) the SAPCTS.

F2.13 The Panel shall, as soon as reasonably practicable after it makes a change to such matrix, notify all the Parties that a change has been made.

Firmware Information Repository

F2.14 The Panel shall establish and maintain a list of firmware releases, updates, and corresponding Manufacturer contact details (the **“Firmware Information Repository”**), for the following Devices:

(a) ESME

(b) GSME

(c) PPMID

(d) HCALCS

(e) SAPC

(f) SMETS1 CH or SMETS2+ Communications Hub

F2.15 The Panel shall ensure that the Firmware Information Repository contains a minimum of four fields:

(a) A number which uniquely identifies a record on the Central Products List, which is a mandatory field;

(b) Manufacturer contact details, which is a mandatory field, to include email address, telephone number and business address;

(c) A free text field for release notes that Manufacturers can record against, which is a mandatory field for completion but the content is at the discretion of the Manufacturer; and

(d) Where a firmware upgrade to the Device Model identified by (a) is possible, the number(s) of the records(s) on the Central Products List which identify the suitable baseline Device Model(s), which is a mandatory field.

F2.16 The Firmware Information Repository will be updated alongside the Central Products List, with the number which uniquely identifies a record on the Central Products List providing a cross reference.

F2.17 The Party or any other person submitting Device details for addition to the Central Products List shall also supply the details listed in F2.15 for the same Device.

F2.17B The information contained within the Firmware Information Repository shall be available to SEC Parties only and must not be shared.

Device Trials

F2.18 The Security Sub-Committee shall consider applications from Manufacturers for SMETS2+ Device Models to be added to the Central Products List, on a limited trial basis, without a CPA Certificate needing to be issued by the NCSC. If approved by the Security Sub-Committee, the relevant SMETS2+ Device Model will be known as a "**Trial Device Model**" for the duration set out in the approval (the " **Trial Device Approval**"). The Security Sub-Committee shall have sole discretion in deciding whether to grant a Trial Device Approval.

F2.19 In its application for Trial Device Approval, the applicant Manufacturer must evidence that the SMETS2+ Device Model for which it is seeking approval has all Assurance Certificates other than a CPA Certificate issued by the NCSC.

F2.20 The Security Sub-Committee shall require a business rationale to support the application, a security risk assessment, and assurance that Energy Consumers of Trial Device Models shall be required to opt into trial participation and informed of the implications of doing so, and may (at its sole discretion) set additional requirements that must be evidenced in an application.

F2.21 Where a Trial Device Approval is granted, the Security Sub-Committee shall set out in a written notice to the Manufacturer and the Panel:

(a) a detailed description of the Trial Device Model;

(b) a summary of why the Trial Device Approval is being granted and the assessment undertaken by the Security Sub-Committee in considering the application;

(c) the start date and expiry date of the Trial Device Approval;

(d) the maximum number of Devices of the Trial Device Model that may be deployed; and

(e) any other conditions applied to the Trial Device Approval.

F2.22 The Security Sub-Committee shall determine the appropriate level of detail to be provided in the Trial Device Approval notice and shall not be required to disclose any information it considers sensitive.

F2.23 If one or more of the conditions applicable to the Trial Device Model are breached, then the Trial Device Approval may be withdrawn or cancelled by the Security Sub-Committee.

F2.24 Where an application is not approved, the Security Sub-Committee shall set out in a written notice to the Manufacturer and the Panel a summary of why approval has not been granted and the assessment undertaken in considering the application. The Security Sub-Committee shall determine the appropriate level of detail to be provided in the summary and shall not be required to disclose any information it considers sensitive.

F2.25 A Trial Device Model will be deemed to have a valid CPA Certificate for the duration of the Trial Device Approval. The Security Sub-Committee shall issue a trial certificate (the "**Trial Device Certificate**") for the duration of the trial in lieu of the CPA Certificate that would ordinarily be issued by the NCSC. The Trial Device Certificate will include an identifier code which is unique to the Trial Device Model and the Trial Device Approval as well as an expiry date which matches the expiry date of the Trial Device Approval. The Trial Device Certificate will be provided to the Manufacturer and the Panel.

F2.26 In respect of a Trial Device Model, this Code will be construed such that any requirement for a SMETS2+ Device Model to have a CPA Certificate shall be deemed satisfied by a valid Trial Device Certificate. Where necessary, the requirements of this Code applicable to a CPA Certificate will be construed so as to not inhibit the use of a Trial Device Model in accordance with a Trial Device Approval and Sections F2.18 to F2.32.

F2.27 With effect from the start date set out in the Trial Device Approval, the Panel shall add the Trial Device Model to the Central Products List. The Central Products List must show that the relevant SMETS2+

Device Model is a Trial Device Model, identify the specific Trial Device Approval that applies to the Trial Device Model, and include the expiry date for such approval.

F2.28 On a monthly basis, the DCC shall provide the Security Sub-Committee with a copy of the Smart Metering Inventory so that the Security Sub-Committee can extract details of Trial Device Models.

F2.29 The Manufacturer of a Trial Device Model may apply to the Security Sub-Committee to request an amendment to its Trial Device Approval. The Security Sub-Committee may amend a Trial Device Approval at any time and at its sole discretion, irrespective of whether an amendment application has been made by the Manufacturer. If the Security Sub-Committee amends a Trial Device Approval, it shall notify the Manufacturer and the Panel. The notice will include a summary of why the Trial Device Approval has been amended. The Security Sub-Committee shall determine the appropriate level of detail to be provided and shall not be required to disclose any information it considers sensitive. Where necessary, the Panel shall update the Central Products List to reflect such amendment.

F2.30 The Security Sub-Committee may withdraw or cancel a Trial Device Approval at any time and at its sole discretion. Upon such withdrawal or cancellation, the Security Sub-Committee shall notify the Manufacturer and the Panel. The notice will include a summary of why the Trial Device Approval has been withdrawn or cancelled. The Security Sub-Committee shall determine the appropriate level of detail to be provided and shall not be required to disclose any information it considers sensitive.

F2.31 If a Trial Device Approval expires, or is withdrawn or cancelled, the Trial Device Certificate will expire, be withdrawn or be cancelled (as applicable) by the Security Sub-Committee and the provisions of Clause 6 (Removal of Device Models from the List) of Appendix Z shall apply in determining whether or not to remove the Trial Device Model from the Central Products List and whether a Trial Device Remedial Plan is to be imposed. If it is determined that the Trial Device Model shall be removed from the Central Products List, the Manufacturer may either apply for a new Trial Device Approval or apply for a CPA Certificate.

F2.32 Where a Trial Device Model is removed from the Central Products List, all Devices of the relevant SMETS2+ Device Model must be promptly Decommissioned by the Responsible Supplier, unless:

(a) the relevant SMETS2+ Device Model has since gained a CPA Certificate (or a new Trial Device Certificate) and has been updated accordingly on the Central Products List; or

(b) the relevant Device can be (and is) updated via firmware to become a SMETS2+ Device Model which is listed on the Central Products List.

Device Zigbee Information Repository

F2.33 The Panel shall establish and maintain a list of Device Zigbee releases, updates and corresponding Manufacturer contact details (the "Device Zigbee Information Repository").

F2.34 The Panel shall ensure that the Device Zigbee Information Repository contains a minimum of three fields:

(a) Zigbee chipset vendor, which is a mandatory field;

(b) Zigbee stack version, which is a mandatory field; and

(c) Central Product List entry ID.

F2.35 The Device Zigbee Information Repository will be updated alongside the Firmware Information Repository and the Central Products List, with the number which uniquely identifies a record on the Firmware Information Repository and the Central Products List providing a cross reference.

F2.36 The Device Zigbee Information Repository will include the Central Products List entry ID to allow the Data in the Device Zigbee Information Repository to be mapped to the Device on the Central Product List.

F2.37 The Party or any other person submitting Device details for addition to the Central Products List shall also supply the details listed in F2.15 for the same Device.

F2.38 The Security Sub-Committee shall manage the access to the Device Zigbee Information Repository.

F3. PANEL DISPUTE RESOLUTION ROLE

F3.1 Where a Party considers that a device which is required under the Energy Licences to meet the requirements of the Technical Specifications does not meet the applicable requirements of the Technical Specifications, then that Party may refer the matter to the Panel for its determination. For the purposes of this Section F3, the relevant licence requirements are Condition 39 of the Electricity Supply Licences, Condition 33 of the Gas Supply Licences, and Condition 17, Part E of the DCC Licence.

F3.2 The devices to which this Section F3 applies need not form part of Enrolled Smart Metering Systems.

F3.3 The DCC shall retain evidence to demonstrate that the Communications Hubs (as defined in the DCC Licence) meet the DCC's obligations under the DCC Licence to ensure compliance with the CHTS. The DCC shall make that evidence available to the Panel or the Authority on request.

F3.4 Save to the extent the DCC is responsible under Section F3.3, each Supplier Party shall retain evidence to demonstrate that the Devices for which it is responsible under the Energy Licences for ensuring Technical Specification compliance do so comply. Each Supplier Party shall make that evidence available to the Panel or the Authority on request.

F3.5 Where the Panel determines that any device or devices that were intended to meet the requirements of a Technical Specification do not meet the applicable requirements of the Technical Specification, the Panel may (to the extent and at such time as the Panel sees fit, having regard to all the circumstances and any representations made by any Competent Authority or any Party) require the relevant Supplier Party or the DCC (as applicable under Section F3.3 or F3.4) to give effect to a reasonable remedial plan designed to remedy and/or mitigate the effect of such non-compliance within a reasonable timescale.

F3.6 Where a Party disagrees with any decision of the Panel made pursuant to Section F3.5, that Party may refer the matter to the Authority for its determination, which shall be final and binding for the purposes of this Code.

F3.7 Subject to any determination by the Authority pursuant to Section F3.6, where the Panel requires a Supplier Party to give effect to a remedial plan in accordance with Section F3.5 and where that Supplier Party fails in a material respect to give effect to that remedial plan, then such failure shall constitute an Event of Default for the purposes of Section M8 (Suspension, Expulsion and Withdrawal).

F3.8 For the avoidance of doubt, no decision of the Panel pursuant to this Section F3 is intended to fetter the discretion of the Authority to enforce any breach of any Energy Licence.

F4. OPERATIONAL FUNCTIONALITY, INTEROPERABILITY AND ACCESS

Operational Functionality

F4.1 The Responsible Supplier for each Enrolled Smart Metering System shall ensure that the Smart Metering System (excluding the Communications Hub Function) is not configured in a way that restricts the minimum functions that the Smart Metering System is required to be capable of providing in order that the DCC can provide the Services in accordance with this Code.

F4.1A The Lead Supplier for a SMETS1 CH shall take all reasonable steps to ensure that the SMETS1 CHF forming part of that SMETS1 CH is not configured in a way that restricts the minimum functions that any Smart Metering System of which the SMETS1 CHF forms part is required to be capable of providing in order that the DCC can provide the Services in accordance with this Code.

F4.1B Subject to Section F4.1C, where the Lead Supplier for a SMETS1 CH upgrades the firmware for or replaces the SMETS1 CHF and/or SMETS1 GPF comprising that SMETS1 CH, then the Lead Supplier shall take reasonable steps to ensure that the upgraded/replacement SMETS1 CHF and/or SMETS1 GPF is compatible with any and all other Devices that formed part of a Smart Metering System of which the SMETS1 CHF and/or SMETS1 GPF that have been upgraded/replaced also formed part. For the purposes of this Section F4.1B, 'compatible' means that the Devices are of Device Models identified as a combination of Device Models in the then current SMETS1 Eligible Product Combinations.

F4.1C The obligation under Section F4.1B is subject to the Lead Supplier's obligations under its Energy Supply Licence with respect to the installation and maintenance of Smart Metering Systems (as defined in its Energy Supply Licence).

Interoperability of SMETS2+ Communications Hubs with DCC Systems

F4.2 Pursuant to the DCC Licence, the DCC has certain obligations to ensure that SMETS2+ Communications Hubs are interoperable with the DCC Systems.

F4.3 Save to the extent the DCC is responsible as described in Section F4.2, the Responsible Supplier for each Enrolled Smart Metering System (but not SMETS1 SMSs) shall ensure that all the Devices forming part of that Smart Metering System are interoperable with the DCC Total System to the extent necessary to enable those Devices to respond to Commands received from or via the DCC in accordance with the requirements defined in the GB Companion Specification.

F4.4 The DCC and each Supplier Party shall:

(a) ensure that testing has been undertaken to demonstrate its compliance with the obligations set out in or referred to in Section F4.2 or F4.3 (as applicable); and

(b) retain evidence of such testing, and make such evidence available to the Panel and the Authority on request.

Remote Access by DCC

F4.5 Subject to Section F4.5A, the Responsible Supplier for each Enrolled Smart Metering System shall ensure that the DCC is allowed such remote access to the Smart Metering System as is reasonably necessary to allow the DCC to provide the Services and any other services permitted by the DCC Licence in respect of that Smart Metering System (including the right to send communications to, to interrogate, and to receive communications and obtain Data from that Smart Metering System).

F4.5A In the case of SMETS1 CHs, the Supplier Party or Supplier Parties which own or are renting the SMETS1 CH (which may or may not be the Responsible Supplier) shall be obliged to comply with Section F4.5 in respect of the SMETS1 CH.

Physical Access to Devices by Parties

F4.6 Where a Party is expressly required or permitted by this Code to interfere with a SMETS2+ Communications Hub, then the DCC hereby consents to the Party interfering with that Communications Hub in that way (and shall ensure that all persons with a legal interest in the Communications Hub have also so consented).

F4.7 Where a User is expressly required by this Code to interfere with a Device forming part of a Smart Metering System (other than the Devices comprising a SMETS2+ Communications Hub), then the Party which owns that Device (or has made arrangements with its owner for its provision) hereby consents to the User interfering with that Device in that way (and shall ensure that all persons with a legal interest in that Device have also so consented).

Communications with Communications Hubs by DCC over the SM WAN

F4.8 Except where expressly permitted or obliged by this Code, the DCC shall ensure that the only Devices with which it communicates over the SM WAN are those listed in the Smart Metering Inventory. Where a Communications Hub Function or Gas Proxy Function has an SMI Status of ‘suspended’, the DCC shall only initiate a communication with that Device (where it is the target device) if following the successful execution of such communication the DCC can reasonably expect that the associated Communication Hub’s Device Model will become one that is listed on the Central Product List.

F4.9 Except in the circumstances described in Section F4.9B, where the DCC receives a Power Outage Event (AD1) Alert from a Communications Hub Function indicating that no power supply has been available to that Communications Hub Function for a period of at least three minutes, the DCC shall send a copy of the Alert to the Import Supplier (if any) and Electricity Distributor (if any) for that Communications Hub Function.

F4.9A The DCC shall maintain a list of Devices which are known to cause a Communications Hub Function to send a Power Outage Event (AD1) Alert for a short period (of greater than three minutes) following commencement of a firmware update.

F4.9B In relation to Devices on such list, in the case of a Power Outage Event (AD1) Alert being received by the DCC within the period of 30 minutes following commencement of a firmware update, the DCC shall not send a copy of the Alert to the Import Supplier or the Electricity Distributor (but the DCC shall record and store details of the Alert, including its suppression in accordance with this Section F4.9B).

SMETS2+ Communications Hub Procurement

F4.10 The DCC shall publish on the DCC Website the physical dimensions of the Communications Hub Device Models that are made available from time to time pursuant to the Communications Hub Services.

F4.11 Within the relevant period established in accordance with this Section F4.11, the DCC shall consult the other Parties regarding the physical dimensions of the Communications Hub Device Models first made available pursuant to the Communications Hub Services (and shall give due consideration to any consultation responses received when considering the Communications Hubs to be made available in the future). For the purposes of this Section F4.11, the relevant period is the period of 18 months (or such shorter period as the Panel may determine) after the date from which Smart Meters are capable of being Commissioned pursuant to Section H5 (Smart Metering Inventory and Enrolment Services).

F4.12 Prior to committing to the procurement of any Communications Hubs comprising:

(a) HAN Variants and/or WAN Variants that have not previously been made available pursuant to the Communications Hub Services; and/or

(b) Communications Hubs with physical dimensions that differ from the physical dimensions of any Communications Hubs that are (at the time of such proposed procurement) made available pursuant to the Communications Hub Services,

the DCC shall consult the other Parties regarding the physical dimensions of the Communications Hubs to be procured (and shall give due consideration to any consultation responses received).

F4.13 Prior to committing to any arrangements (or any changes to arrangements) for the financing of any Communications Hub procurement, the DCC shall, to the extent such arrangements (or changes) might reasonably be expected to have a material effect on one or more of the other Parties, consult with the other Parties regarding the same. Such consultation shall include the DCC's explanation of how the arrangements (or changes) are consistent with the requirements of the DCC Licence and this Code.

F4.14 In respect of each Dual Band Communications Hub that the DCC delivers pursuant to Section F6 (Delivery and Acceptance of Communications Hubs), the DCC shall ensure that the data items stored on the Communications Hub are (at the time of delivery) configured in accordance with the requirements of the DCC Dual Band Communications Hub Configuration Table.

F4.15 In respect of each Smart Metering System which includes a Dual Band Communications Hub, the Lead Supplier from time to time shall ensure that the data items stored on the Communications Hub are (at all times) configured in accordance with the requirements of the Lead Party Dual Band Communications Hub Configuration Table.

Preventing Unauthorised Access to Data

F4.16 The DCC and each other Party that is responsible from time to time for the risk of loss or destruction of or damage to a SMETS2+ Communications Hub shall take reasonable steps to ensure that Personal Data held on that Communications Hub is protected from unauthorised access during such period of responsibility.

F4.17 The Lead Supplier from time to time for each SMETS1 CH shall take reasonable steps to ensure that Personal Data held on that SMETS1 CH is protected from unauthorised access.

Annex to Section F4 - Dual Band Communications Hub Configuration Tables

Each data item in the first column is to be configured in accordance with third column.

DCC Dual Band Communications Hub Configuration Table

Data item	Reference	Default Value
Page 28 Mask	GBCS v2.0 Table 10.6.2.3	channels 0 to 26
Page 29 Mask	GBCS v2.0 Table 10.6.2.3	channels 27 to 34
Page 30 Mask	GBCS v2.0 Table 10.6.2.3	channels 35 to 48
Page 31 Mask	GBCS v2.0 Table 10.6.2.3	no channels to be used
Normal-Limited Duty Cycle Threshold	GBCS v2.0 Table 10.6.2.3	2.0%
Limited-Critical Duty Cycle Threshold	GBCS v2.0 Table 10.6.2.3	2.4%
Maximum Sub GHz Channel Changes Per Week	GBCS v2.0 Table 10.6.2.3	2 per week
GSME Curfew	GBCS v2.0 Table 10.6.2.3	5 hours
Channel Quieter Threshold	GBCS v2.0 Table 10.6.2.3	3 dB
Channel Noisier Threshold	GBCS v2.0 Table 10.6.2.3	3 dB
Non GSME Poor Communications Percentage Threshold	GBCS v2.0 Table 10.6.2.3	20%
Non GSME Poor Communications Thirty Minute Periods Measurement Periods	GBCS v2.0 Table 10.6.2.3	50 periods
Local CH Noise Measurement Period	GBCS v2.0 Table 10.6.2.3	2 hours
Local CH Failure Percentage	GBCS v2.0 Table 10.6.2.3	10%
Local CH Retry Percentage	GBCS v2.0 Table 10.6.2.3	30%

Lead Party Dual Band Communications Hub Configuration Table

Data item	Reference	Default Value
Page 28 Mask	GBCS v2.0 Table 10.6.2.3	channels 0 to 26
Page 29 Mask	GBCS v2.0 Table 10.6.2.3	channels 27 to 34
Page 30 Mask	GBCS v2.0 Table 10.6.2.3	channels 35 to 48
Page 31 Mask	GBCS v2.0 Table 10.6.2.3	no channels to be used
Normal-Limited Duty Cycle Threshold	GBCS v2.0 Table 10.6.2.3	2.0%
Limited-Critical Duty Cycle Threshold	GBCS v2.0 Table 10.6.2.3	2.4%
Maximum Sub GHz Channel Changes Per Week	GBCS v2.0 Table 10.6.2.3	2 per week

GSME Curfew	GBCS v2.0 Table 10.6.2.3	5 hours
Channel Quieter Threshold	GBCS v2.0 Table 10.6.2.3	3 dB
Channel Noisier Threshold	GBCS v2.0 Table 10.6.2.3	3 dB
Non GSME Poor Communications Percentage Threshold	GBCS v2.0 Table 10.6.2.3	20%
Non GSME Poor Communications Thirty Minute Periods Measurement Periods	GBCS v2.0 Table 10.6.2.3	50 periods
Local CH Noise Measurement Period	GBCS v2.0 Table 10.6.2.3	2 hours
Local CH Failure Percentage	GBCS v2.0 Table 10.6.2.3	10%
Local CH Retry Percentage	GBCS v2.0 Table 10.6.2.3	30%

F5. SMETS2+ COMMUNICATIONS HUB FORECASTS & ORDERS

All references to "Communications Hubs" in this Section F5 are references to "SMETS2+ Communications Hubs".

Availability of CH Variants

F5.1 The DCC shall ensure that Communications Hub Device Models are made available to be ordered by Parties under this Section F5 such that the Parties can order Communications Hubs that provide for each and every combination of HAN Variant and WAN Variant; save that:

(a) this Section F5 does not apply to Special Installation Mesh Communications Hubs (and all references in this Section F5 to Communications Hubs shall be deemed to exclude Special Installation Mesh Communications Hubs); and

(b) the DCC need not provide a 'Variant 450 Communications Hub' (as defined in the CH Installation and Maintenance Support Materials) that operates only with a HAN frequency within the 2400 – 2483.5 MHz harmonised frequency band (as further described in the CHTS).

Temporary CH Ordering and Delivery Rules

F5.1A The provisions of the Section F5 (and the definitions defined by reference to this Section F5) shall apply in accordance with (and subject to) any and all variations applied from time to time under a document to be known as the "**Temporary CH Ordering and Delivery Rules**". The DCC shall produce and obtain the Panel's approval of the Temporary CH Ordering and Delivery Rules, setting out the variations to this Section F5 that are reasonably required as a consequence of global supply chain issues or other reasonable adjustments that might be needed. The DCC may from time to time amend the Temporary CH Ordering and Delivery Rules, the DCC shall consult with Parties and any amendments shall be subject to the Panel's approval, and in accordance with any procedure for amendments set out in the rules. The Temporary CH Ordering and Delivery Rules will include an end date for any requirement, or set of requirements, and any extension must be made in accordance with Section F5.1A.

Communications Hub Forecasts

F5.2 For the purposes of this Section F5, a "**Communications Hub Forecast**" means an estimate of the future requirements of a Party for the delivery to it of Communications Hubs by the DCC, which:

(a) is submitted by that Party to the DCC;

(b) covers the period identified in Section F5.3; and

(c) complies with the requirements of Section F5.4.

F5.3 Each Communications Hub Forecast shall cover the period of 12 months commencing with the sixth month after the end of the month in which the forecast is submitted to the DCC.

F5.4 Each Communications Hub Forecast shall:

(a) comprise a forecast of the number of Communications Hubs that the Party requires to be delivered to it in each month of the period to which it relates;

(b) set out that forecast for each such month by reference to:

(i) the aggregate number of Communications Hubs to be delivered;

(ii) the number of Communications Hubs to be delivered in respect of each Region; and

(iii) the number of Communications Hubs of each HAN Variant to be delivered in respect of each Region ; and

(c) include such further information and be provided in such form as may be set out in the CH Handover Support Materials at the time of its submission.

Parties: Duty to Submit Communications Hub Forecasts

F5.5 Each Supplier Party, and each other Party that intends to order Communications Hubs in the future, shall:

(a) submit a Communications Hub Forecast to the DCC by no later than the 5th Working Day prior to the last Working Day of each month;

(b) submit each Communications Hub Forecast via the CH Ordering System;

(c) take reasonable steps to ensure that the information contained in each Communications Hub Forecast is accurate and up to date; and

(d) ensure that it submits a forecast that will enable it to submit a Communications Hub Order that meets the requirements of Section F5.12.

F5.6 A Party that has not submitted a Communications Hub Forecast for a Region during a month in accordance with this Section F5 shall be deemed to have submitted a forecast which specified the same number of Communications Hubs as the Party forecast or is deemed to have forecast for the previous month.

Communications Hub Orders

F5.7 For the purposes of this Section F5, a "**Communications Hub Order**" means an order by a Party for the delivery to it of Communications Hubs and/or Communications Hub Auxiliary Equipment by the DCC, which:

(a) is submitted by that Party to the DCC; and

(b) satisfies the requirements of Section F5.8.

F5.8 Each Communications Hub Order shall (subject to any further requirements set out in the CH Handover Support Materials):

(a) relate to a single Region, and identify the Region to which it relates;

(b) relate to the delivery of Communications Hubs and/or Communications Hub Auxiliary Equipment in the 5th month after the end of the month in which that Communications Hub Order is submitted to the DCC (the "**Delivery Month**");

(c) specify the addresses of the location or locations (each a "Delivery Location") at which the delivery of the Communications Hubs and/or Communications Hub Auxiliary Equipment is required, each of which locations must be in Great Britain but need not be in the Region to which the relevant Communications Hub Order relates;

(d) specify, in accordance with Section F5.12, the number (if any) of Communications Hubs of each Device Model to be delivered to each Delivery Location (in each case, a **"Delivery Quantity"**);

(e) specify the preferred date within the Delivery Month on which the delivery to each Delivery Location is required (provided that the actual delivery date within the Delivery Month for each Delivery Location (in each case, a "**Delivery Date**") shall be determined in accordance with the CH Handover Support Materials);

(f) specify the number and type of the Communications Hub Auxiliary Equipment (if any) to be delivered to each Delivery Location; and

(g) include such further information and be provided in such form as may be set out in the CH Handover Support Materials at the time of its submission.

F5.9 In respect of each Communications Hub Order submitted in respect of a Region, the Communications Hubs and/or Communications Hub Auxiliary Equipment to be delivered to each Delivery Location on each Delivery Date shall be a "**Consignment**".

F5.10 In order for a Communications Hub Order to be a compliant order, the order must comply with the requirements of this Section F5.10. A Party is not obliged to submit a compliant order, but a non-compliant order may be amended by the DCC in accordance with Section F5.17. The requirements of this Section F5.10 are, for each Communications Hub Order submitted by a Party in respect of a Region, that the aggregate (for all Consignments) of the Delivery Quantities of each HAN Variant for the Delivery Month must be:

(a) greater than or equal to the higher of 80% of the number of Communications Hubs of that HAN Variant forecast for that Delivery Month and Region in the Communications Hub Forecast submitted by that Party in the 12th month prior to the start of the Delivery Month; and

(b) less than or equal to the lower of 120% of the number of Communications Hubs of that HAN Variant forecast for that Delivery Month and Region in the Communications Hub Forecast submitted by that Party in the 12th month prior to the start of the Delivery Month.

F5.11 For the purposes of Section F5.10, in calculating, by reference to earlier forecast numbers:

(a) the minimum aggregate of the Delivery Quantities, any fractions of a number shall be rounded down; and

(b) the maximum aggregate of the Delivery Quantities, any fractions of a number shall be rounded up.

F5.12 For each Party's Communications Hub Order relating to a Region, the aggregate of the Delivery Quantities (for all Device Models taken together) that may be specified for each Consignment may not (unless such number is zero) be less than the minimum delivery quantity set out in the CH Handover Support Materials at the time at which the relevant Communications Hub Order is submitted.

Parties: Rights and Duties in relation to Communications Hub Orders

F5.13 Each Party other than the DCC:

(a) may submit one Communications Hub Order in relation to each Region in any month;

(b) shall submit a Communications Hub Order in relation to a Region in a month if the aggregate of the Delivery Quantities for one or more Device Models required for a compliant order in accordance with Section F5.10 is greater than zero; and

(c) where it fails to submit an order where it is required to do so in accordance with Section F5.13(b), shall be deemed to have submitted a Communications Hub Order for a Delivery Quantity of Communications Hubs of each Device Model equal to the minimum aggregate Delivery Quantity required in respect of that Device Model for a compliant order in accordance with Section F5.10 (and the remaining details of such deemed order shall be determined by the DCC in accordance with the CH Handover Support Materials).

F5.14 Each Party shall ensure that any Communications Hub Order which it elects or is required to submit in any month is submitted by no later than the 5th Working Day prior to the last Working Day of that month.

F5.15 Each Party shall submit its Communications Hub Orders via the CH Ordering System.

DCC: Duties in relation to Communications Hub Orders

F5.16 Where the DCC receives a Communications Hub Order from a Party via the CH Ordering System, the DCC shall:

(a) promptly acknowledge receipt of that order; and

(b) within five Working Days of its receipt of the order, notify the Party either that:

(i) the order satisfies the requirements of Section F5.8, is a compliant order in accordance with Section F5.10 and was submitted in accordance with Section F5.14 (and is therefore accepted); or

(ii) the order does not satisfy some or all of the conditions in (i) above (and is therefore subject to Section F5.17).

F5.17 Where this Section F5.17 applies in respect of a Party's Communications Hub Order, the DCC shall (having regard to the nature, extent and effect of the Party's breach of this Section F5 and/or of the order's non-compliance under Section F5.10, and having regard to the requirements of the DCC Licence) take all reasonable steps to accommodate the order (in whole or part, or subject to amendments). The DCC shall, by the end of the month in which such order is received by the DCC, notify the Party (in each case giving reasons for its decision) that:

(a) the order is accepted in its entirety;

(b) the order is accepted in part or subject to amendment; or

(c) the order is rejected.

DCC Policy

F5.18 The DCC shall develop and make available via the DCC Website a policy describing the circumstances in which it will accept (in whole or part, or subject to amendments) or reject Communications Hub Orders as described in Section F5.17.

Non-Standard Cancellation of Consignments

F5.19 Each Party that has had a Communications Hub Order accepted by the DCC may cancel one or more of the Consignments arising from that Communications Hub Order; provided that the Party must notify the DCC of such cancellation at least 48 hours in advance of the Delivery Date for the Consignment. A Party which cancels one or more Consignments in accordance with this Section F5.19 shall be liable to reimburse the DCC for all reasonable costs and expenses incurred by the DCC as a result of such cancellation. The DCC shall notify the Party of such costs and expenses as soon as reasonably practicable after notice of the cancellation is given. Such compensation shall be included in the next Invoice to be produced by the DCC following its calculation. The DCC shall, where requested not less than 10 Working Days in advance of the Delivery Date, provide a non-binding estimate of the costs and expenses it is likely to incur in the event that a Party opts to cancel a Consignment (such estimate to be provided not less than 5 Working Days in advance of the Delivery Date). The DCC shall take all reasonable steps to ensure the estimate is accurate.

CH Ordering System

F5.20 Subject to Section F5.23, the DCC shall make one or more systems (the **CH Ordering System**) available to other Parties, which Parties can access remotely (via such means, and subject to any security requirements, as are set out in the CH Support Materials).

F5.21 The DCC shall ensure that the CH Ordering System is available in advance of the time from which other Parties are obliged to submit Data via the CH Ordering System, and at all times thereafter (subject to Planned Maintenance undertaken in accordance with Section H8.3).

F5.22 The DCC shall ensure that the CH Ordering System allows each Party to:

(a) submit details of its forecasts, orders and returns of Communications Hubs and/or Communications Hub Auxiliary Equipment, as required in accordance with this Section F5, Sections F6 (Delivery and Acceptance of Communications Hubs) and F8 (Removal and Return of Communications Hub), and the CH Support Materials;

(b) view Data regarding the status of such submissions (but only its own submissions), and (where relevant) receive responses from the DCC regarding such submissions; and

(c) view the SM WAN Coverage Database.

CH Order Management System Accounts

F5.23 The DCC may, as further described in the CH Support Materials:

(a) limit the number of accounts via which each Party is able to access the CH Order Management System without paying any additional Charges; and

(b) allow each Party additional accounts via which it is able to access the CH Order Management System, subject to such Party agreeing to pay the applicable Charges.

F6. DELIVERY AND ACCEPTANCE OF SMETS2+ COMMUNICATIONS HUBS

All references to "Communications Hubs" in this Section F6 are references to "SMETS2+ Communications Hubs".

Delivery

F6.1 The DCC shall ensure that the applicable numbers of Communications Hub Products are delivered in accordance with Valid Communications Hubs Orders to the relevant Delivery Location on the relevant Delivery Date during the relevant Delivery Window.

F6.2 The DCC shall ensure that the Communications Hub Products are delivered in accordance with the delivery requirements set out in the CH Handover Support Materials.

F6.3 The Party assigned responsibility for doing so under the CH Handover Support Materials shall ensure that the Communications Hub Products are unloaded from the delivery vehicle at the Delivery Location in accordance with Good Industry Practice and the CH Handover Support Materials.

F6.4 Delivery of Communications Hub Products pursuant to this Code shall occur on removal of the Communications Hub Products from the delivery vehicle at the Delivery Location (subject to any additional requirements in the CH Handover Support Materials).

F6.5 Risk of loss or destruction of or damage to the Communications Hub Products shall transfer to the Party which submitted the Communications Hub Order on commencement of their unloading at the Delivery Location (where not unloaded by the DCC) or on completion of their unloading at the Delivery Location (where unloaded by the DCC).

F6.6 Notwithstanding delivery, legal and beneficial ownership of the Communications Hub Products shall at all times (for the purposes of this Code) remain vested in the DCC, subject only to Section F7.10 (Ownership of and Responsibility for Communications Hub Auxiliary Equipment).

Confirmation of Delivery

F6.7 The Party which submitted the Valid Communications Hub Order shall confirm whether or not a delivery of Communications Hub Products has been made in compliance with the order within five days after the applicable Delivery Date (such confirmation to be submitted in accordance with and contain the information specified in the CH Handover Support Materials and via the CH Ordering System).

F6.8 Where a Party fails to submit a confirmation in accordance with Section F6.7, the Party shall be deemed to have confirmed that a delivery of Communications Hub Products has been made in compliance with the relevant order.

F6.9 The only grounds for non-compliance under Section F6.7 are that:

(a) no delivery was made to the relevant Delivery Location on the relevant Delivery Date, or the delivery was made but contained fewer Communications Hub Products of the applicable Device Model or type than the DCC was obliged to deliver;

(b) the delivery contained more Communications Hub Products of the applicable Device Model or type than the DCC was obliged to deliver to the relevant Delivery Location on the relevant Delivery Date;

(c) the delivered Communications Hub Products are (or reasonably appear on a visual inspection to be) damaged or have been (or reasonably appear on a visual inspection to have been) tampered with (and such damage or tampering occurred prior to their delivery to the Party as described in Section F6.4); and/or

(d) the Party is otherwise entitled to reject the Communications Hub Products in accordance with the CH Handover Support Materials.

Rejected Communications Hub Products

F6.10 Where a Party notifies the DCC under Section F6.7 that a delivery is non-compliant in accordance with Sections F6.9(b), (c) and/or (d), the Party thereby rejects the Communications Hub Products in question.

F6.11 Where Section F6.10 applies, the Party to which the rejected Communications Hub Products were delivered shall make those Communications Hub Products available for collection by the DCC in accordance with the CH Handover Support Materials.

F6.12 The Party assigned responsibility for doing so under the CH Handover Support Materials shall ensure that the rejected Communications Hub Products are loaded on to the DCC's vehicle in accordance with Good Industry Practice and the CH Handover Support Materials. Risk of loss or destruction of or damage to such Communications Hub Products shall transfer to the DCC on commencement of such loading (where loaded by the DCC) or on completion of such loading (where not loaded by the DCC).

Replacement Communications Hub Products

F6.13 Where a Party notifies the DCC under Section F6.7 that a delivery is non-compliant in accordance with Sections F6.9(a), (c) and/or (d), the DCC shall ensure that replacement Communications Hub Products of the applicable Device Model or type and in the number necessary to make up the shortfall are delivered to the relevant Delivery Location as soon as reasonably practicable thereafter.

F6.14 Where Section F6.13 applies, the DCC shall (via the CH Ordering System) notify the Party of the dates on which the DCC is able to deliver such replacement Communications Hub Products, and this Section F6 shall apply as if:

(a) the replacement Communications Hub Products to be delivered pursuant to this Section F6.14 were the subject of a Valid Communications Hub Order; and

(b) the date selected by the Party, out of the dates so notified by the DCC, was the Delivery Date for that order.

Access to Delivery Location

F6.15 The Party which submitted the Communications Hub Order shall ensure that each of the DCC and its sub-contractors and its and their agents is allowed access to the Delivery Location for the purposes of exercising the DCC’s rights and performing the DCC’s obligations under this Section F6.

F6.16 The DCC shall ensure that each person that accesses a Delivery Location pursuant to Section F6.15 shall do so in compliance with Good Industry Practice and the site rules and reasonable instructions of the relevant Party (or its representatives).

Non-Standard Delivery Options

F6.17 Each Party which submits a Communications Hub Order may specify non-standard delivery instructions where and to the extent provided for in the CH Handover Support Materials. Subject to such Party agreeing to pay any applicable Charges, the DCC shall comply with such delivery instructions.

Failure to Accept Delivery

F6.18 Where the Party which submitted a Valid Communications Hub Order breaches its obligations under this Section F6 and/or the CH Handover Support Materials and as a result the DCC is not able to deliver the Communications Hub Products in accordance with this Code, that Party shall be liable to reimburse the DCC for all reasonable costs and expenses incurred by the DCC as a result. The DCC shall notify the Party of such costs and expenses as soon as reasonably practicable after the event. Such compensation shall be included in the next Invoice to be produced by the DCC following its calculation.

Special Installation Mesh Communications Hubs

F6.19 Special Installation Mesh Communications Hubs are not ordered under Section F5 (Communications Hub Forecasts & Orders). Consequently, Special Installation Mesh Communications Hubs are not delivered under this Section F6. All references in this Section F6 to Communications Hubs shall be deemed to exclude Special Installation Mesh Communications Hubs.

Timing of CHTS Compliance

F6.20 The DCC is obliged under the DCC Licence to deliver Communications Hubs that are within their Installation Validity Period and is thereafter subject to licence obligations relating to their maintenance. Nothing in this Section F6 (or elsewhere in this Code) is intended to require the DCC to ensure CHTS compliance at the time of a Communications Hub's installation.

F6A. TRANSFERRING COMMUNICATIONS HUBS BETWEEN PARTIES

All references to "Communications Hubs" in this Section F6A are references to "SMETS2+ Communications Hubs".

Communications Hub Transfers

F6A.1 Each Party shall be able to take a transfer of Communications Hubs from a Party that is not the DCC (a **"Communications Hub Transfer"**) in accordance with this Section F6A.

Communications Hub Transfer Request

F6A.2 A **"Communications Hub Transfer Request"** means a request by a Party (referred to as the requesting Party) for a Communications Hub Transfer, which request:

(a) is submitted by the requesting Party to the DCC via email to the applicable address published by the DCC on the DCC Website; and

(b) specifies the number of Communications Hubs of each Device Model to be transferred.

F6A.3 Where the DCC receives a Communications Hub Transfer Request from a Party, the DCC shall promptly:

(a) acknowledge receipt of that request; and

(b) notify all Parties which are at that time in receipt of Communications Hubs of the requested Device Model(s) which have not yet been installed or transferred.

F6A.4 Each Party (referred to as the transferring Party) that wishes to transfer Communications Hubs to the requesting Party shall, within 10 Working Days of the DCC's notification, notify the DCC via email of:

(a) the number of Communications Hubs available to transfer to the requesting Party;

(b) whether or not the proposed transfer is capable of acceptance in part (for some only of the Communications Hubs available for transfer);

(c) the addresses of the location or locations (each a "**Transfer Location**") at which collection of the Communications Hubs is required, each of which locations must be in Great Britain; and

(d) the preferred date on which the collection from each Transfer Location is required (a **"Transfer Date"**), which date is subject to change in accordance with the CH Handover Support Materials.

F6A.5 The DCC shall:

(a) where one or more notifications is received in accordance with Section F6A.4, provide such information by email to the requesting Party; and

(b) where the DCC does not receive notifications in accordance with Section F6A.4, reject the Communications Hub Transfer Request and notify the requesting Party of such rejection by email.

F6A.6 Where a notification has been received in accordance with Section F6A.5(a), the requesting Party shall notify DCC by email whether the requesting Party accepts, accepts in part (where permitted), or rejects the prospective Communications Hub Transfer. Where the DCC does not receive such notification within 10 Working Days of DCC's communication under Section F6A.5(a), then the requesting Party will be deemed to have rejected the prospective Communications Hub Transfer.

F6A.7 Where a Communications Hub Transfer has been accepted or (if permitted) accepted in part by the requesting Party in accordance with Section F6A.6, then a binding Communications Hub Transfer shall be created.

Communications Hub Transfer

F6A.8 Where a binding Communications Hub Transfer is created under Section F6A.7, the requesting Party and the transferring Party (assisted by the DCC) shall ensure that the Communications Hubs in question are transferred in accordance with the transfer requirements set out in the CH Handover Support Materials.

F6A.9 The requesting Party shall ensure that the Communications Hubs are loaded on to the collection vehicle at the Transfer Location in accordance with Good Industry Practice and the CH Handover Support Materials.

F6A.10 Transfer of Communications Hubs pursuant to this Code shall occur on loading of the Communications Hubs on to the collection vehicle at the Transfer Location (subject to any additional requirements in the CH Handover Support Materials).

F6A.11 Risk of loss or destruction of or damage to the Communications Hubs shall transfer to the requesting Party on commencement of their unloading at the Transfer Location.

F6A.12 Notwithstanding delivery, legal and beneficial ownership of the Communications Hubs shall at all times (for the purposes of this Code) remain vested in the DCC.

Confirmation of Transfer

F6A.13 The requesting Party shall confirm to the DCC whether or not a transfer of Communications Hubs has been made in compliance with the Communications Hub Transfer Request within one day after the applicable Transfer Date (such confirmation to be submitted in accordance with and to contain the information specified in the CH Handover Support Materials).

F6A.14 Where a requesting Party fails to submit a confirmation in accordance with Section F6A.13, the DCC shall contact the requesting Party, and the requesting Party shall confirm in accordance with Section F6A.13.

Rejection of Communications Hub Transfers

F6A.15 Once a binding Communications Hub Transfer is created under Section F6A.7, the only grounds on which the requesting Party can reject some or all of the Communications Hubs covered by that Communications Hub Transfer are that:

(a) those Communications Hubs (of the applicable Device Model) were not available for collection from the Transfer Location on the Transfer Date;

(b) the Communications Hubs are (or reasonably appear on a visual inspection to be) damaged or have been (or reasonably appear on a visual inspection to have been) tampered with (and such damage or tampering occurred prior to transfer of risk under Section F6A.11); and/or

(c) the Party is otherwise entitled to reject Communications Hubs in accordance with the CH Handover Support Materials.

F6A.16 Where the requesting Party rejects some or all of the Communications Hubs covered by a Communications Hub Transfer in accordance with Section F6A.15 risk and responsibility for those Communications Hubs shall not transfer to the requesting Party and they shall remain the risk and responsibility of the transferring Party.

F7. INSTALLATION AND MAINTENANCE OF SMETS2+ COMMUNICATIONS HUBS

All references to "Communications Hubs" in this Section F7 are references to "SMETS2+ Communications Hubs".

Installation

F7.1 Each Supplier Party that installs a Communications Hub shall ensure that such Communications Hub is installed in accordance with the CH Installation and Maintenance Support Materials.

F7.2 Where:

(a) a Supplier Party is installing a Communications Hub for a premises; and

(b) the Supplier Party knows (or should reasonably know) that the premises will also require a Communications Hub Function to form part of a Smart Metering System with a Smart Meter for which the Supplier Party is not a Responsible Supplier,

then that Supplier Party shall, to the extent that it is reasonably able to do so, install a Communications Hub such that the Communications Hub Function will be capable of forming part of a Smart Metering System with both the Smart Meter for which it is a Responsible Supplier and the Smart Meter for which it is not a Responsible Supplier.

F7.3 On completion of the installation of a Communications Hub in accordance with Section F7.1, risk of loss or destruction of or damage to the Communications Hub shall cease to vest in the Party in which risk previously vested, which will either have been the Party which ordered the Communications Hub or the Party which obtained the Communications Hub under a Communications Hub Transfer (or, in the case of Special Installation Mesh Communications Hubs, shall cease to vest in the Supplier Party which took delivery of the Communications Hub).

Risk in the Communications Hubs following Installation

F7.4 Following completion of installation of a Communications Hub, risk of loss or destruction of or damage to the Communications Hub shall vest in the same or a different Party as follows:

(a) where the Communications Hub is removed from a premises by a Supplier Party, then the risk of loss or destruction of or damage to that Communications Hub shall vest in that Supplier Party such that that Supplier Party is responsible for all such risk since installation of the Communication Hub until such risk transfers to the DCC under Section F8.11 (Acceptance of a Returned Communications Hub); or

(b) where a Communications Hub is lost or destroyed following completion of its installation at a premises and before commencement of its removal from a premises by a Supplier Party, then the Supplier Party that is obliged to notify the DCC of a Communications Hub's loss or destruction under Section F8.17(b) (Loss or Destruction of Communications Hubs) shall be deemed to bear the risk of such loss or destruction.

Special Installation Mesh Communications Hubs

F7.4A Where it is determined in accordance with the CH Installation and Maintenance Support Materials that a Supplier Party is required to install a Special Installation Mesh Communications Hub in respect of a premises, then the following provisions shall apply:

(a) the DCC shall (subject to Section F7.5) deliver a Special Installation Mesh Communications Hub to the Supplier Party at the premises;

(b) the DCC shall ensure that the Special Installation Mesh Communications Hub that is delivered is of the HAN Variant that the Supplier Party requests;

(c) delivery, risk and ownership of the Special Installation Mesh Communications Hub shall be subject to the same principles as are described in Sections F6.5 and F6.6 (Delivery) by reference to the Supplier Party to which the Communications Hub is handed by the DCC and completion of such hand over (as completion of handover is further described in the CH Handover Support Materials);

(d) following delivery of a Special Installation Mesh Communications Hub as referred to in this Section F7.4A, the Special Installation Mesh Communications Hub shall be subject to the provisions of this Section F7 and of Sections F8 (Removal and Return of Communications Hubs) and F9 (Categories of Communications Hub Responsibility), save as otherwise expressly provided;

(e) in addition to the application of Section F8 (Removal and Return of Communications Hubs), a Supplier Party may return a Special Installation Mesh Communications Hub to the DCC while the Supplier Party and the DCC are still at the premises to which the Communications Hub was delivered, by handing the Communications Hub to the DCC (and the DCC shall accept handover of the Communications Hub, at which point risk of loss or destruction of or damage to the Communications Hub shall transfer to the DCC);

(f) without prejudice to the other obligations of the DCC and the Responsible Suppliers under this Code in respect of Communications Hubs installed at premises, where a Responsible Supplier reasonably determines that an Incident is likely to require replacement or repair of the SIMCH Aerial, then the DCC shall (subject to Section F7.5) attend the premises and (where necessary) undertake such replacement or repair; and

(g) each SIMCH Aerial shall be subject to Section F7.9 as if it was Communications Hub Auxiliary Equipment, save that no Party other than the DCC may replace or repair a SIMCH Aerial.

Special Installations & Modifications

F7.5 Where the CH Installation and Maintenance Support Materials require the DCC to undertake works on behalf of a Supplier Party, and where such works require the consent or agreement of any person other than the Supplier Party or the DCC (including where the consent or agreement of the Energy Consumer and/or any landlord or other owner of premises is required), then that Supplier Party shall ensure that such consent or agreement is obtained in advance (and the DCC shall provide all information reasonably requested by the Supplier Party in relation to it obtaining such consent or agreement).

F7.6 A Supplier Party responsible under Section F7.5 for obtaining a consent or agreement in relation to works shall take reasonable steps to obtain such consent or agreement in a form that permits the installation, operation, repair, modification, replacement and removal of the equipment.

F7.7 Where the DCC attends any premises and/or undertakes any works in reliance on a consent or agreement obtained (or required to be obtained) by a Supplier Party under Section F7.5, the DCC shall do so:

(a) as the contractor of that Supplier Party;

(b) in accordance with Good Industry Practice, the applicable consent or agreement obtained pursuant to Section F7.5 (and notified to the DCC), and the site rules and reasonable instructions of the owner and/or occupier of the relevant premises;

(c) in compliance with all Laws and/or Directives applicable to the Supplier Party or its representatives (and notified to the DCC), including the requirements of the Supplier Party's Energy Licence concerning Supplier Party representatives who attend premises; and

(d) in compliance with all reasonable requests of the Supplier Party.

F7.8 Not used

Ownership of and Responsibility for Communications Hub Auxiliary Equipment

F7.9 In respect of those types of Communications Hub Auxiliary Equipment that are designed to be installed at premises, such Communications Hub Auxiliary Equipment shall be deemed to form part of the Communications Hub, and the provisions of this Section F7 and of Sections F8 (Removal and Return of Communications Hubs) and F9 (Categories of Communications Hub Responsibility) shall be construed accordingly.

F7.10 In respect of those types of Communications Hub Auxiliary Equipment to which Section F7.9 does not apply:

(a) legal and beneficial ownership of such Communications Hub Auxiliary Equipment shall vest in the Party that ordered it on risk in such equipment transferring to that Party under Section F6.5 (Delivery); and

(b) legal and beneficial ownership of such Communications Hub Auxiliary Equipment shall (where applicable) revert to the DCC on risk in such equipment transferring to the DCC under Section F6.12 (Rejected Communications Hub Products).

CH Support Materials Compliance and Access to Premises

F7.11 The DCC shall reply to any reasonable request from a Party for information pertaining to compliance by the DCC with the CH Support Materials.

F7.12 Each Party shall reply to any reasonable request from the DCC for information pertaining to compliance by that Party with the CH Support Materials.

F7.13 Where the DCC wishes to attend a premises at which a Communications Hub is installed in order to assess a Party's compliance with the CH Support Materials in respect of that Communications Hub, the DCC may request access from the Responsible Supplier for the Smart Metering System(s) of which the Communications Hub forms part (or, where there is more than one such Responsible Supplier, from either or both of them as further described in the CH Support Materials).

F7.14 Where a Responsible Supplier consents to a request under Section F7.13, the Responsible Supplier shall take all reasonable steps to obtain the consent of the Energy Consumer to the DCC attending the premises.

F7.15 Where a Responsible Supplier does not consent to a request under Section F7.13, the DCC may refer the matter to the Panel. The Panel shall determine whether it is reasonably necessary for the DCC to attend the premises in order to assess (in general) a Party's compliance with the CH Support Materials. Where the Panel determines that it is, the Responsible Supplier shall take all reasonable steps to obtain the consent of the Energy Consumer to the DCC attending the premises.

F7.16 Where the Energy Consumer's consent is obtained pursuant to Section F7.14 or F7.15, the Responsible Supplier and the DCC shall follow the relevant procedure for attending the premises set out in the CH Support Materials.

F7.17 Where the DCC attends any premises in reliance on a consent obtained by a Supplier Party pursuant to Section F7.14 or F7.15, the DCC shall do so:

(a) as the contractor of that Supplier Party;

(b) in accordance with Good Industry Practice, the applicable consent (as notified to the DCC), and the site rules and reasonable instructions of the owner and/or occupier of the relevant premises;

(c) in compliance with all Laws and/or Directives applicable to the Supplier Party or its representatives (and notified to the DCC), including the requirements of the Supplier Party’s Energy Licence concerning Supplier Party representatives who attend premises; and

(d) in compliance with all reasonable requests of the Supplier Party.

Resolution of SMETS2+ SM WAN Coverage Incidents

F7.18 Where a Communications Hub is installed at a premises in accordance with this Code but does not connect to the SM WAN, and the SM WAN Coverage Database indicated (at any time during the 30 days prior to the date of installation) that the SM WAN is (or would be) available in the area in which the premises is located on the installation date, then the DCC shall (within 90 days after having been notified in accordance with the CH Installation and Maintenance Support Materials):

(a) provide a response to the installing Supplier Party that either (i) confirms that the SM WAN is now available in the relevant area such that Communications Hubs installed at premises in that area can be expected to be able to connect to the SM WAN; or (ii) provides reasons why the SM WAN is not so available; and

(b) (subject to Section F7.20) ensure that, in the case of at least 99% of all Communications Hubs for which the DCC is required to give such a response in each calendar quarter, the SM WAN is made available in the relevant area such that Communications Hubs installed at premises in that area can be expected to be able to connect to the SM WAN (but excluding for this purpose those locations where SM WAN connectivity is affected by problems with access pursuant to Section F7.5 which arise otherwise than as a result of the DCC's breach of this Code).

F7.19 Where a Communications Hub is installed at a premises in accordance with this Code but does not connect to the SM WAN (in circumstances where Section F7.18 does not apply), and the SM WAN Coverage Database is updated after installation to indicate that the premises is within an area in which the SM WAN is available, then (provided the DCC has been notified of the installation in accordance30with the CH Installation and Maintenance Support Materials) the DCC shall (within 90 days after such update occurs):

(a) provide a response to the Supplier Party which installed the Communications Hub that either (i) confirms that the SM WAN is now available in the relevant area such that Communications Hubs installed at premises in that area can be expected to be able to connect to the SM WAN; or (ii) provides reasons why the SM WAN is not so available; and

(b) (subject to Section F7.20) ensure that, in the case of at least 99% of all Communications Hubs for which the DCC is required to give such a response in each calendar quarter, the SM WAN is available in the relevant area such that Communications Hubs installed at premises in that area can be expected to be able to connect to the SM WAN (but excluding for this purpose those locations where SM WAN connectivity is affected by problems with access pursuant to Section F7.5 which arise otherwise than as a result of the DCC's breach of this Code).

F7.20 Until 1 January 2021, Sections F7.18(b) and F7.19(b) do not apply to Communications Hubs installed at premises within a geographic area that is subject to a Network Enhancement Plan. Such Communications Hubs shall, until 1 January 2021, be excluded from the calculations under Sections F7.18(b) and F7.19(b).

F7.21 Within a reasonable period of time following each calendar quarter that ends prior to 1 January 2021, the DCC shall produce a report which identifies:

(a) any new Network Enhancement Plans that have been created during that quarter, any Network Enhancement Plans that were completed during that quarter, and any ongoing Network Enhancement Plans; and

(b) for each such Network Enhancement Plan:

(i) an overview of the geographic area that is subject to the plan;

(ii) the premises (by postcode) that fall within that area; and

(iii) the scheduled date for completion of the planned works (or, where applicable, the actual date of completion).

F7.22 A copy of the report produced under Section F7.21 shall be provided by the DCC to the Parties, the Panel, the Authority and (on request) the Secretary of State.

F8. REMOVAL AND RETURN OF SMETS2+ COMMUNICATIONS HUBS

All references to "Communications Hubs" in this Section F8 are references to "SMETS2+ Communications Hubs".

Product Recall / Technology Refresh

F8.1 The DCC's rights under this Section F8.1 are in addition to (and separate from) the rights of the DCC (and the obligations of the other Parties) to remove and/or return Communications Hubs under other provisions of this Code (including pursuant to the Incident Management Policy and the CH Support Materials). The DCC has the right to request (in reliance on this Section F8.1) that Parties return to the DCC one or more Communications Hubs. Following receipt of such a request:

(a) in respect of Communications Hubs that have been delivered but have not yet been installed at premises, the Party which ordered those Communications Hubs shall return them to the DCC (or, if there has been a Communications Hub Transfer, the Party which obtained the Communications Hub under the Communications Hub Transfer);

(b) in respect of Communications Hubs that have been installed at premises and not yet removed from that premises, the Lead Supplier for those Communications Hubs shall remove them from the premises and return them to the DCC (and this obligation shall apply whether or not such Lead Supplier is a User); and

(c) in respect of Communications Hubs that have been removed from a premises and not yet returned to the DCC, the Supplier Party that removed the Communications Hub from the premises shall return them to the DCC.

F8.2 Where Section F8.1 applies, the DCC shall provide to Supplier Parties all such information as they or their Energy Consumers reasonably require in respect of the situation. Those Supplier Parties to whom Section F8.1(b) applies shall issue to affected Energy Consumers such information as is provided by the DCC concerning the situation.

Removal of Communications Hubs

F8.3 Each Supplier Party that:

(a) is a Responsible Supplier for the Communications Hub Function forming part of a Communications Hub, is entitled to remove that Communications Hub from the premises at which it is installed (but must install a replacement Communications Hub);

(b) Decommissions a Communications Hub Function, shall remove the Communications Hub of which the Communications Hub Function forms part from the premises at which it is installed; and

(c) is a Responsible Supplier for the Communications Hub Function forming part of a Communications Hub, may also be obliged under another provision of this Code to remove a Communications Hub, including where it is obliged to do so in accordance with the Incident Management Policy or the CH Support Materials.

F8.4 Where a Supplier Party removes a Communications Hub from a premises, it shall do so in accordance with the CH Installation and Maintenance Support Materials.

F8.5 Where a Communications Hub is removed by a Supplier Party from a premises at which it was previously installed, then the risk of loss or destruction of or damage to that Communications Hub shall vest in that Supplier Party as set out in Section F7.4(a) (Risk in the Communications Hubs following Installation).

Return of Communications Hubs

F8.6 Where a Communications Hub is removed by a Supplier Party from a premises at which it was previously installed, the Supplier Party shall return the Communications Hub to the DCC within 90 days after the date of its removal. This obligation to return a Communications Hub only applies where the Communications Hub Function which forms part of that Communications Hub has at any time had an SMI Status of 'installed not commissioned' or 'commissioned'.

F8.7 A Party that wishes to return a Communications Hub to the DCC shall be entitled to do so at any time. A Party that ceases to be a Party shall return to the DCC all the Communications Hubs that have been delivered to that Party and not yet: (a) transferred under a Communications Hub Transfer; (b) installed at premises; or (c) reported as lost or destroyed.

F8.8 The DCC shall publish on the CH Ordering System the following information:

(a) the addresses of no more than two locations in respect of each Region to which Communications Hubs can be returned (which locations must be in Great Britain), making clear which Device Models may be returned to which locations;

(b) the operating hours of each such location during which returns can be made (which operating hours must be reasonable); and

(c) any changes to the information required to be published under (a) and (b) above, for which at least four months' advance notice must be given (unless the Panel approves a shorter period).

F8.9 A Party required or opting to return one or more Communications Hubs to the DCC shall:

(a) notify the DCC of the number of Communications Hubs to be returned, of the location to which they are to be returned (being one of the locations published for the relevant Region in accordance with Section F8.8), of the date on which they are to be returned, and of any further information required in accordance with the CH Installation and Maintenance Support Materials;

(b) return those Communications Hubs to the location and on the date notified in accordance with (a) above during the applicable operating hours for that location published in accordance with Section F8.8;

(c) otherwise comply with the return requirements set out in the CH Installation and Maintenance Support Materials; and

(d) be liable to pay the applicable Charges in the event that it returns one or more Communications Hubs to the wrong returns location.

Acceptance of Returned Communications Hubs

F8.10 The Party assigned responsibility for doing so under the CH Handover Support Materials shall ensure that the returned Communications Hubs are unloaded from the vehicle in which they have been returned, and that they are unloaded in accordance with Good Industry Practice and the CH Installation and Maintenance Support Materials.

F8.11 Risk of loss or destruction of or damage to returned Communications Hubs shall transfer to the DCC on commencement of such unloading (where unloaded by the DCC) or on completion of such unloading (where not unloaded by the DCC).

Access to Returns Locations

F8.12 The DCC shall ensure that each Party (and its sub-contractors and its and their agents) is allowed access to the locations published pursuant to Section F8.8 for the purposes of exercising the Party's rights and performing the Party's obligations under this Section F8.

F8.13 The relevant Party shall ensure that any person that accesses a location pursuant to Section F8.14 shall do so in compliance with Good Industry Practice and the site rules and reasonable instructions of the DCC (or its representatives).

Reconditioning or Disposal of Communications Hubs by the DCC

F8.14 The DCC shall take all reasonable steps to recondition and redeploy each Communications Hub that is returned to the DCC (having regard to the requirements of the DCC Licence).

F8.15 Before a Communications Hub that has been returned to the DCC is delivered to a Party pursuant to Section F6 (Delivery and Acceptance of Communications Hubs), the DCC shall ensure that all Data relating to one or more Energy Consumers is permanently erased from that Communications Hub in accordance with the standard referred to in Section G2.18 (Management of Data).

F8.16 Unless the Communications Hub is reconditioned and redeployed in accordance with Sections F8.14 and F8.15, the DCC shall ensure that each Communications Hubs that has been returned to the DCC is disposed of in accordance with Good Industry Practice and the standard referred to in Section G2.18 (Management of Data).

Loss or Destruction of Communications Hubs

F8.17 Where a Communications Hub has been lost or destroyed (save where such loss or destruction occurs while the risk of loss or destruction was the responsibility of the DCC), the following Party shall notify the DCC of such loss or destruction (via the CH Ordering System):

(a) where such loss or destruction occurs prior to completion of the Communications Hub’s installation at a premises by a Supplier Party, the Party that ordered that Communications Hub (or, in the case of Special Installation Mesh Communications Hubs, the Supplier Party which took delivery of the Communications Hub);

(b) where such loss or destruction occurs after completion of such installation and before commencement of the Communications Hub's removal from a premises by a Supplier Party, the Supplier Party responsible under the Incident Management Policy for resolving the relevant Incident; or

(c) where such loss or destruction occurs after commencement of the Communications Hub's removal from a premises by a Supplier Party, the Supplier Party which undertook such removal.

F8.18 Where a Communications Hub is lost or destroyed following completion of its installation at a premises by a Supplier Party and before commencement of its removal from a premises by a Supplier Party, then the Supplier Party that is obliged to notify the DCC of such loss or destruction under Section F8.17(b) shall be deemed to bear the risk of such loss or destruction as described in Section F7.4(b) (Risk in the Communications Hubs following Installation Installation).

F9. CATEGORIES OF SMETS2+ COMMUNICATIONS HUB RESPONSIBILITY

All references to "Communications Hubs" in this Section F9 are references to "SMETS2+ Communications Hubs".

Overview

F9.1 The reason for the return of each returned Communications Hub, or for its loss or destruction, shall be determined in accordance with this Section F9.

F9.2 The Party which returns a Communications Hub to the DCC shall specify the reason for the Communications Hub's return. The Party which notifies the DCC of a Communications Hub's loss or destruction shall specify the reason it was lost or destroyed. In any such case, such Party shall specify the reason in accordance with the CH Support Materials.

F9.3 The reason specified by the relevant Party pursuant to Section F9.2 shall be subject to any contrary determination in accordance with this Section F9.

F9.4 The reason for the return of a Communications Hub, as finally determined in accordance with this Section F9, shall be used to determine the applicable category of responsibility (as described in Section F9.4), which is then used for the purposes of calculating the Charges (or adjustments to the Charges in accordance with this Section F9).

Reasons

F9.5 The reasons that apply for the purposes of this Section F9 are as follows:

(a) [not used];

(b) return of a Communications Hub to the DCC due to a Special Second-Fuel Installation;

(c) return of a Communications Hub to the DCC due to a Special WAN-Variant Installation;

(d) loss or destruction of or damage to a Communications Hub, which occurred while the relevant Party was responsible for such risk and which was caused otherwise than by a breach of this Code by the DCC or a CH Defect;

(e) return of a Communications Hub to the DCC, other than where another reason under this Section F9.5 applies;

(f) that the Communications Hub has a CH Defect;

(g) loss or destruction of or damage to a Communications Hub caused by a breach of this Code by the DCC;

(h) rejection of a Communications Hub in accordance with Section F6.10 (Rejected Communications Hub Products); and

(i) return of a Communications Hub to the DCC where requested by the DCC under Section F8.1 (Product Recall / Technology Refresh).

Categories of Responsibility

F9.6 For the purposes of this Section F9 and the Charging Methodology:

(a) each of the reasons described in Sections F9.5(d) and (e) constitute a "**CH User Responsibility**", and where the Party required to do so under Section F9.2 fails to specify a reason in accordance with that Section the reason shall be deemed to be a CH User Responsibility;

(b) each of the reasons described in Sections F9.5(f) and (g) (where they apply prior to completion of the installation of the Communications Hub at a premises in accordance with the CH Installation and Maintenance Support Materials) and Section F9.5(h) constitute a "**CH Pre-Installation DCC Responsibility**";

(c) each of the reasons described in Sections F9.5(f) and (g) (where they apply following completion of the installation of the Communications Hub at a premises in accordance with the CH Installation and Maintenance Support Materials) constitute a "**CH Post-Installation DCC Responsibility**";

(d) the reason described in Sections F9.5(i) constitute a "**Product Recall or Technology Refresh**"; and

(e) the reasons described in Sections F9.5(b) and (c) do not need to be categorised, as they do not directly give rise to a Charge or an adjustment to the Charges under this Section F9.

CH Fault Diagnosis

F9.7 The DCC has the right to examine and test returned Communications Hubs and to investigate the cause of any damage to or loss or destruction of Communications Hubs to verify whether the reason given by a Party pursuant to Section F9.2 is correct (being "**CH Fault Diagnosis**").

F9.8 The DCC shall undertake CH Fault Diagnosis in accordance with the process for the same described in the CH Installation and Maintenance Support Materials (which may include sampling and extrapolation of results based on sampling).

F9.9 The DCC shall, within 10 days after the return of Communications Hubs or notification of their loss or destruction by a Party, notify that Party (via the CH Ordering System) if the DCC intends to undertake any CH Fault Diagnosis in respect of those Communications Hub.

F9.10 In the absence of a notification in accordance with Section F9.9, the reason given by a Party in accordance with Section F9.2 in respect of the Communications Hubs in question shall be deemed to be correct.

F9.11 Provided the DCC has first given notice in accordance with Section F9.9, where the DCC disputes the reason given by a Party pursuant to Section F9.2 in respect of any Communications Hubs, the DCC shall provide to the Party a report setting out the DCC's analysis of why the reason given by the Party is not correct.

F9.12 Where the DCC does not provide a report to the Party in accordance with Section F9.11 within 35 days after the DCC's notice to a Party under Section F9.9, the reason given by the Party in accordance with Section F9.2 in respect of the Communications Hubs in question shall be deemed to be correct.

F9.13 Unless the Party notifies the DCC of the Party's objection to the DCC's analysis within 35 days after receipt of a report in accordance with Section F9.11, the analysis set out in the report shall be deemed to be correct.

F9.14 Where the Party notifies the DCC of an objection within the time period required by Section F9.13, then either of them may refer the matter to the Panel for determination (which determination shall be final and binding for the purposes of this Code). Where the Panel is unable to determine the reason for a

Communications Hub's return, then the reason given by the relevant Party under Section F9.2 shall be deemed to be correct.

Reporting on DCC Faults

F9.15 The DCC shall report to the Panel and the other Parties on the number of Communications Hubs for which the reason for return, loss or destruction is determined in accordance with this Section F9 to have been a CH Pre-Installation DCC Responsibility or a CH Post-Installation DCC Responsibility. The DCC shall report in respect of successive periods of three months (starting with the month in which Communications Hubs are first delivered pursuant to this Section F). Such report shall include a supporting explanation of the circumstances that gave rise to such instances of CH Pre-Installation DCC Responsibility or CH Post-Installation DCC Responsibility. Where the DCC is disputing (under CH Fault Diagnosis) whether an instance of CH Pre-Installation DCC Responsibility or CH Post-Installation DCC Responsibility has arisen, the DCC shall not include those instances until the matter is finally resolved (under CH Fault Diagnosis).

Compensation for CH Type Faults

F9.16 Where the reason for a Communications Hub’s return, loss or destruction is determined in accordance with this Section F9 to have been a CH Post-Installation DCC Responsibility, then a “CH Type Fault”shall be said to have occurred in respect of that Communications Hub (at the time of such return or notification, and in respect of the Party making such return or notification).

F9.17 Section F9.18 shall apply in respect of a Region and a calendar year, where the number of CH Type Faults relating to that Region and occurring during that calendar year exceeds 0.5% of the total number of Communications Hubs that are installed at premises within that Region as at the end of that calendar year.

F9.18 Where this Section F9.18 applies in respect of a Region and a calendar year, the DCC shall be liable to pay to Parties collectively an amount of liquidated damages equal to the positive amount (if any) calculated as follows:

(a) £50.00; multiplied by

(b) the Consumer Prices Index for April of that calendar year, divided by the Consumer Prices Index for September 2013; multiplied by

(c) (i) the number of CH Type Faults relating to that Region and occurring during that calendar year; less (ii) 0.5% of the total number of Communications Hubs that are installed at premises within that Region as at the end of that calendar year; less (iii) the number of CH Type Faults relating to that Region and occurring during that calendar year for which the DCC is liable to pay a CH Batch Fault Payment.

F9.19 The aggregate amount (if any) payable by the DCC under Section F9.18 in respect of a Region and a calendar year shall be payable by the DCC to each Party (the amount payable to each Party being a “**CH Type Fault Payment**”) pro-rated in proportion to:

(a) the number of CH Type Faults (across all Regions) which occurred in respect of that Party during that calendar year, less the number of CH Type Faults (across all Regions) which occurred in respect of that Party during that calendar year for which the DCC is liable to pay a CH Batch Fault Payment; as compared to

(b) the total number of CH Type Faults (across all Regions) which occurred in respect of all Parties during that calendar year, less the number of CH Type Faults (across all Regions) which occurred in respect of all Parties during that calendar year for which the DCC is liable to pay a CH Batch Fault Payment.

Compensation for Batch Faults

F9.20 A "**CH Batch Fault**" shall occur in respect of a Delivery Batch where:

(a) the number of CH Type Faults which occur in respect of a Communications Hub forming part of that Delivery Batch, and which occur within 12 months following completion of the installation of that Communications Hub; exceeds

(b) 10% of the number of Communications Hubs comprising that Delivery Batch.

F9.21 Where a CH Batch Fault occurs in respect of a Delivery Batch, the DCC shall be liable to pay to each Party an amount of liquidated damages (being a "**CH Batch Fault Payment")** equal to:

(a) £50.00; multiplied by

(b) the Consumer Prices Index for April of that calendar year, divided by the Consumer Prices Index for September 2013; multiplied by

(c) the number of CH Type Faults which occurred in respect of that Party and a Communications Hub which formed part of that Delivery Batch, and which occur within 12 months following completion of the installation of that Communications Hub.

Payment of Type Fault and Batch Fault Compensation

F9.22 The DCC shall include each CH Type Fault Payment and each CH Batch Fault Payment payable to a Party as a credit in favour of that Party under the DCC's Invoices (so as to reduce the Charges payable by that Party).

Compensation for Product Recall or Technology Refresh

F9.23 Where the reason for a Communications Hub's return is determined in accordance with this Section F9 to have been a Product Recall or Technology Refresh, then the DCC shall (notwithstanding Section M2.8 (Exclusion of Other Liabilities)) be liable to each other Party for the reasonable costs and expenses incurred by that Party in:

(a) any corrective action taken by that Party in accordance with this Code or other Laws and/or Directives (including any withdrawal or recall activities); and/or

(b) notifying or warning Energy Consumers of any corrective action taken by the DCC and/or any other Party (and providing Energy Consumers with relevant information regarding such corrective action).

Damage Caused by Defective Communications Hubs

F9.24 Where a CH Defect causes loss of or damage to physical property (including loss of or damage to Systems, and loss or corruption of Data), such loss or damage shall be deemed to have been caused by a breach of this Code by the DCC, including for the purposes of M2.5 (Damage to Physical Property).

Exclusive Remedies for Site Visits

F9.25 Notwithstanding Sections F9.24 and M2.6(a) (Recovery of Loss which is Expressly Permitted), no Party shall be entitled to recover from the DCC any costs or expenses incurred in attending a premises for the purposes of repairing or replacing any Devices damaged or destroyed as a result of a CH Defect. This Section F9.25 is without prejudice to the CH Type Fault Payments, CH Batch Fault Payments, and compensation under Section F9.23 in respect of Product Recall or Technology Refresh.

Exclusive Remedy for Damaged or Lost Communications Hubs

F9.26 No Party shall have any liability to the DCC for damage to, or loss or destruction of, Communications Hubs. This Section F9.26 is without prejudice to the Charges payable in respect of the Communications Hub Services.

F10. SMETS2+ TEST COMMUNICATIONS HUBS

Overview

F10.1 Unless expressly stated otherwise, the references in this Code to Communications Hubs do not include Test Communications Hubs.

F10.2 Without limiting the generality of Section F10.1, because Test Communications Hubs are not to be treated as Communications Hubs, Test Communications Hubs shall:

(a) not be included in Communications Hub Forecasts or Communications Hub Orders;

(b) not be subject to Sections F5 (Communications Hub Forecasts & Orders) to F9 (Categories of Communications Hub Responsibility);

(c) not be (or be capable of being) Commissioned; and

(d) only be populated with Test Certificates (and not actual Organisation Certificates or Device Certificates).

Prototype Communications Hubs

F10.3 Where the DCC provides a Prototype Communications Hub as a Test Communications Hub (in accordance with the definition of Test Communications Hub), the DCC shall provide details of the manner in which the Prototype Communications Hub does not comply with CHTS. For the purposes of this Section F10.3 and the definition of Prototype Communications Hub, until such time as the CHTS forms part of this Code, the references to the CHTS shall be construed by reference to the draft of the CHTS that the Secretary of State directs from time to time for the purposes of this Section F10.3.

Provision of Test Communications Hubs

F10.4 The DCC shall provide Test Communications Hubs to other Parties and to any other person that requests them (in each case in accordance with the other provisions of this Section F10).

F10.5 Where a person that is not a Party wishes to order Test Communications Hubs, the DCC shall offer terms upon which Test Communications Hubs may be ordered. Such offer shall be provided as soon as reasonably practicable after receipt of the request, and shall be based on the Specimen Enabling Services Agreement (subject only to such variations from such specimen form as are reasonable in the circumstances). A person that is bound by an agreement entered into with the DCC pursuant to this Section F10.5 shall be a "**TCH Participant**". The DCC shall not provide Test Communications Hubs to a person that is not a Party or a TCH Participant.

F10.6 The DCC shall allow Parties and TCH Participants to order and return Test Communications Hubs via a reasonable means.

F10.7 The DCC shall publish on the DCC Website a guide describing the process by which Parties and other persons may obtain and return Test Communications Hubs.

Ordering, Delivery, Rejection and Returns

F10.8 Where a Party or a TCH Participant has ordered one or more Test Communications Hubs via the means described in Section F10.6:

(a) the person that ordered the Test Communications Hubs shall be liable to pay the applicable Charge;

(b) the DCC shall deliver the Test Communications Hubs to the location in Great Britain requested by the person that ordered the Test Communications Hubs, on the date requested by that person (provided that the DCC shall have no obligation to deliver Test Communications Hubs earlier than the date 18 weeks after the date on which the Test Communications Hubs were ordered);

(c) delivery of the Test Communications Hubs shall occur on their removal from the delivery vehicle at the delivery location;

(d) legal and beneficial ownership of (and responsibility for loss or destruction of or damage to) the Test Communications Hubs shall vest in the person that ordered them on commencement of their unloading at the delivery location (where not unloaded by the DCC) or on completion of their unloading at the delivery location (where unloaded by the DCC);

(e) the person that ordered the Test Communications Hubs shall be entitled to reject a delivery and arrange for the return of the rejected Test Communications Hubs to the DCC on the following basis (and only where notified to the DCC within five days of the delivery date):

(i) to the extent the delivery contained more Test Communications Hubs than were ordered; and/or

(ii) to the extent the Test Communications Hub Products are (or reasonably appear on a visual inspection to be) damaged or have been (or reasonably appear on a visual inspection to have been) tampered with (and such damage or tampering occurred prior to their delivery);

(f) the person that ordered the Test Communications Hubs shall be entitled to return them to the DCC where a CH Defect arises within 6 months following their delivery, but not thereafter (for which purpose, the definition of CH Defect shall be construed by reference to the requirements for Test Communications Hubs rather than those for Communications Hubs);

(g) a person wishing to return a Test Communications Hub to the DCC pursuant to (e) or (f) above shall return it to the DCC in accordance with the relevant rules applicable to Communications Hubs under Section F8 (Removal and Return of Communications Hubs); and

(h) legal and beneficial ownership of (and responsibility for loss or destruction of or damage to) the Test Communications Hubs rejected or returned pursuant to this Section F10.8 shall revert to the DCC on completion of their unloading at the returns location (where not unloaded by the DCC) or on commencement of their unloading at the returns location (where unloaded by the DCC).

F10.9 The rejection and/or return of Test Communications Hubs by a Party or TCH Participant pursuant to Section F10.8 is relevant in determining the Charges payable by that Party or TCH Participant. Where the DCC wishes to do so, it may undertake physical and electronic analysis in respect of Test Communications Hubs rejected or returned, in which case the process for CH Fault Diagnosis shall apply, but:

(a) by reference to the reason for rejection and/or return given pursuant to Section F10.6 (rather than by reference to the reason given pursuant to Section F9 (Categories of Communications Hub Responsibility)); and

(b) without the DCC's ability to apply sampling and extrapolation to the extent that such an ability is set out in the CH Installation and Maintenance Support Materials.

Use of Test Communications Hubs

F10.10 The Party or TCH Participant that ordered a Test Communications Hub shall (unless or until it is returned pursuant to Section F10.8) ensure that the Test Communications Hub shall:

(a) only be used by Parties or TCH Participant for the purposes of tests undertaken under this Code, or for the purposes of testing Devices or Systems to be used in relation to this Code; and

(b) be used and maintained in accordance with Good Industry Practice, and the requirements of this Code applicable to Test Communications Hubs.

F10.11 Where a CH Defect in a Test Communications Hub (for which purpose, the definition of CH Defect shall be construed by reference to the requirements for Test Communications Hubs rather than those for Communications Hubs) causes loss of or damage to physical property (including loss of or damage to Systems, and loss or corruption of Data), such loss or damage shall be deemed to have been caused by a breach of this Code by the DCC, including for the purposes of M2.5 (Damage to Physical Property).

Availability of Test CH Variants

F10.12 The DCC shall ensure that the Test Communications Hubs made available pursuant to this Section F10 represent SMETS2+ Communications Hubs that provide for each and every combination of HAN Variant and WAN Variant; subject to Section F10.15.

F10.13 The DCC shall not be obliged to make one or more Test Communications Hub variants available pursuant to this Section F10 where it is not cost effective to do so (having regard to the obligations of Supplier Parties under this Code, including under Section F4.4 (Interoperability with DCC Systems)).

F10.14 Where the DCC seeks to rely on Section F10.13 in respect of one or more variants, the DCC shall publish notice of that fact on the DCC Website, including within such notice the DCC's justification for why it is not cost effective to make that variant available pursuant to this Section F10. Where a Party disagrees with the DCC's justification in respect of one or more variants, that Party may refer the matter to the Panel to determine whether the DCC's justification is valid. Where the DCC or any other Party disagrees with the Panel's determination, the DCC or such other Party may refer the matter to the Authority for its determination (which shall be final and binding for the purposes of this Code).

F10.15 Where the DCC seeks to rely on Section F10.13 in respect of one or more variants, the DCC shall not be obliged to make the Test Communications Hub variant available pursuant to this Section F10 until either:

(a) the Panel has determined that the DCC is obliged to make the variant available, and the DCC has not referred the matter to the Authority within 20 Working Days following the Panel's determination; or

(b) the Authority has determined that the DCC is obliged to make the variant available.

F11. ALCS/HCALCS/APC/SAPC LABELS LIST

ALCS/HCALCS/APC/SAPC Labels List

F11.1 The Panel will establish and maintain a list of ALCS/HCALCS/APC/SAPC labels which provide a standardised naming convention for all possible ALCS, HCALCS, APCs and SAPCs (the " **ALCS/HCALCS/APC/SAPC Labels List**").

F11.2 The Panel will agree updates to the ALCS/HCALCS/APC/SAPC Labels List as proposed by Parties.

F11.3 Within one working day after the ALCS/HCALCS/APC/SAPC Labels List is updated, the Panel will:

(a) publish a copy of the updated list on the website; and

(b) notify the Parties that the list has been updated.

F12. SMART METER DEVICE ASSURANCE SUB-COMMITTEE

Establishment of the Smart Meter Device Assurance Sub-Committee

F12.1 The Panel shall establish a Sub-Committee in accordance with the requirements of this Section F12, to be known as the "**Smart Meter Device Assurance Sub-Committee**" (or SMDA Sub-Committee for short).

F12.2 Save as expressly set out in this Section F12, the SMDA Sub-Committee shall be subject to the provisions concerning Sub-Committees set out in Section C6 (Sub-Committees).

F12.3 Membership of the SMDA Sub-Committee shall be determined by the Panel from time to time in accordance with the following principles:

(a) at the time of its establishment, the SMDA Sub-Committee shall comprise the individuals who are (at that time) performing the equivalent role on behalf of the Smart Meter Device Assurance Company Limited (company number 09327524), but without prejudice to the Panel's powers to subsequently alter the membership; and

(b) otherwise in accordance with Section C6.7 (Membership); save that Section C6.7(b) shall not apply in respect of the individuals appointed to the SMDA Sub-Committee at the time of its establishment.

Role of the SMDA Sub-Committee

F12.4 The two key objectives of the SMDA Sub-Committee shall be (in respect of SMETS2+ Devices only):

(a) to provide assurance that Smart Meters and other Devices which can together potentially form a Smart Metering System work together (that they are interoperable); and

(b) to provide assurance that Smart Meters and other Devices which can together potentially form a Smart Metering System work with each other (that they are interchangeable).

F12.5 In furtherance of these objectives, the SMDA Sub-Committee shall (subject to the terms of reference imposed by the Panel) procure and manage provision of services from one or more independent testing organisations to provide interoperability and interchangeability testing services for SMETS2+ Devices to Supplier Parties, Manufacturers, meter asset providers, and such other entities as the SMDA Sub-Committee may determine from time to time.

F12.6 The SMDA Sub-Committee's duties, powers, functions and procedural rules shall otherwise be determined in accordance with Section C6.10 (Terms of Reference and Procedural Requirements).

F12.7 Not Used

Approach to Service Provision

F12.8 Each testing organisation appointed pursuant to Section F12.5 shall be appointed under a framework agreement entered into by SECCo which enables Supplier Parties, Manufacturers, meter asset providers, and such other entities as the SMDA Sub-Committee may determine from time to time to contract for the testing services available under the framework.

Approach to Cost Recovery

F12.9 Each framework agreement entered into by SECCo pursuant to Section F12.8 shall provide for:

(a) a reasonable amount of fixed costs to be paid by SECCo, which amounts paid by SECCo shall be treated as Recoverable Costs in accordance with Section C8 (Panel Costs and Budgets); and

(b) the incremental costs of providing testing services to a particular Supplier Party, Manufacturer, meter asset provider, or other entity to be charged to that Supplier Party, Manufacturer, meter asset provider, or other entity (and on the basis that SECCo shall not be liable for those incremental costs).

F13. NETWORK EVOLUTION TRANSITION AND MIGRATION APPROACH DOCUMENT

Overview

F13.1 The Network Evolution Transition and Migration Approach Document is to be developed by the DCC pursuant to this Section F13, and incorporated into this Code pursuant to Part G of Condition 22 of the DCC Licence and Section X5 (Incorporation of Certain Documents into this Code).

Purpose of the Network Evolution Transition and Migration Approach Document

F13.2 The purposes of the Network Evolution Transition and Migration Approach Document are to:

(a) enable an orderly and coordinated transition and/or migration to, any or all of the Network Evolution Arrangements; and

(b) provide for additional and/or varied provisions to apply for a transitional period prior to, during and/or following the implementation of any or all of the Network Evolution Arrangements.

Content of the Network Evolution Transition and Migration Approach Document

F13.3 The Network Evolution Transition and Migration Approach Document may include, without limitation, some or all of the following:

(a) rights and/or obligations of the DCC and other Parties designed to facilitate or achieve the purposes of the Network Evolution Transition and Migration Approach Document which are either additional to or vary other rights and/or obligations set out in this Code;

(b) rules and requirements concerning the provision and sharing of Data in order to facilitate or achieve the purposes of the Network Evolution Transition and Migration Approach Document, which may include one or more Parties being obliged to provide (or procure the provision of) Data (as further described in the Network Evolution Transition and Migration Approach Document);

(c) limitations and/or variations to the Services and/or the rights and/or obligations of the Parties to apply for a transitional period prior to and/or following the establishment of any or all of the Network Evolution Arrangements, which may include limitations and/or variations to Services;

(d) the variation of limitations on liability provided for in this Code for a transitional period prior to and/or following the establishment of any or all of the Network Evolution Arrangements;

(e) provision for the referral and determination of disputes in respect of the Network Evolution Transition and Migration Approach Document, which may include interim or final determinations by the Secretary of State, the Authority, the Panel or any other person specified by the Secretary of State.

Process to Develop Document for Designation

F13.4 The DCC shall, to the extent it has not already done so when this Section F13 comes into effect, develop and consult on the first version of the Network Evolution Transition and Migration Approach Document which shall include provisions relating to the CH&N Arrangements and submit it to the Secretary of State in accordance with the following process:

(a) the DCC shall, in consultation with the Parties and such other persons as are likely to be interested, produce a draft of the document;

(b) where a disagreement arises with any Party or other person with regard to any proposal as to the content of the document, the DCC shall endeavour to reach an agreed proposal with that person consistent with the purposes of the Network Evolution Transition and Migration Approach Document;

(c) the DCC shall send a copy of the draft document to the Secretary of State as soon as is practicable after completion of the process described in (a) and (b) above, and shall when doing so provide to the Secretary of State:

(i) a statement of the reasons why the DCC considers that draft to be fit for purpose;

(ii) copies of the consultation responses received; and

(iii) a summary of any disagreements that arose during consultation and that have not been resolved by reaching an agreed proposal; and

(d) the DCC shall comply with any direction given to it by the Secretary of State following the Secretary of State's consideration of the draft document which direction may require the DCC to:

(i) make such amendments to the draft document as are set out or described in the direction;

(ii) produce and submit to the Secretary of State a further draft of the document; and

(iii) follow a specified process (and the time within which that process shall be completed) prior to submitting a further draft of the document to the Secretary of State.

F13.5 The DCC shall, where so directed by the Secretary of State from time to time, develop and consult upon the second (and any subsequent) version of the Network Evolution Transition and Migration Approach Document (which direction may require that version to include provisions relating to one or more of the other parts of the Network Evolution Arrangements) and submit it to the Secretary of State in accordance with the process set out in Section F13.4 and in accordance with any timescales that may be specified in the direction.

Application of the Network Evolution Transition and Migration Approach Document

F13.6 The DCC and the categories of Party referred to in the Network Evolution Transition and Migration Approach Document shall comply with the Network Evolution Transition and Migration Approach Document.

F13.7 The Network Evolution Transition and Migration Approach Document shall have priority over the other provisions of this Code in relation to the subject matter of the Network Evolution Transition and Migration Approach Document.

Expiry of the Network Evolution Transition and Migration Approach Document

F13.8 The Network Evolution Transition and Migration Approach Document shall provide for a date (or a mechanism for determining a date) from which the Network Evolution Transition and Migration Approach Document is to no longer apply. From such date, the Network Evolution Transition and

Migration Approach Document shall no longer have any effect (but without prejudice to the rights and obligations arising prior to that date).

Definitions

F13.9 For the purposes of this Section F13:

CH&N Arrangements	means the arrangements described in subparagraph(a) of the definition of Network Evolution Arrangements.
Network Evolution Arrangements	has the meaning given to that term in Condition13B of the DCC Licence.

G SECURITY

G1. SECURITY: GENERAL PROVISIONS

Interpretation

G1.1 Sections G2 to G9 shall be interpreted in accordance with the following provisions of this Section G1.

Transitional Period for Updated or Replacement Standards

G1.2 Section G1.3 applies where:

(a) the DCC or any User is required, in accordance with any provision of Sections G2 to G9, to ensure that it, or that any of its policies, procedures, systems or processes, complies with:

(i) any standard, procedure or guideline issued by a third party; and

(ii) any equivalent to that standard, procedure or guideline which updates or replaces it from time to time; and

(b) the relevant third party issues an equivalent to that standard, procedure or guideline which updates or replaces it.

G1.3 Where this Section G1.3 applies, the obligation on the DCC or User (as the case may be):

(a) shall be read as an obligation to comply with the updated or replaced standard, procedure or guideline from such date as is determined by the Panel (having considered the advice of the Security Sub-Committee) in respect of that document; and

(b) prior to that date shall be read as an obligation to comply (at its discretion) with either:

(i) the previous version of the standard, procedure or guideline; or

(ii) the updated or replaced standard, procedure or guideline.

G1.4 Any date determined by the Panel in accordance with Section G1.3 may be the subject of an appeal by the DCC or any User to the Authority (whose decision shall be final and binding for the purposes of this Code).

Obligations on Users

G1.5 Obligations which are expressed to be placed on a User shall, where that User performs more than one User Role, be read as applying to it separately in respect of each of its User Roles.

G1.6 For the purposes of Section G1.5, where any Network Party is deemed to have nominated itself as a Registration Data Provider (in accordance with the definition of Registration Data Provider), its role as a Registration Data Provider shall be treated as if it were an additional category of User Role.

Exclusion for Export Suppliers and Registered Supplier Agents

G1.7 Where a User acts in the User Role of 'Export Supplier' or 'Registered Supplier Agent', it is not to be subject to any of the obligations expressed to be placed on Users except for those obligations set out at:

(a) Sections G3.2 to G3.3 (Unauthorised Activities: Duties to Detect and Respond);

(b) Sections G3.8 to G3.9 (Management of Vulnerabilities);

(c) Sections G5.14 to G5.18 (Information Security: Obligations on Users), save that for this purpose the reference:

(i) in Section G5.18(b)(i) to "Sections G3 and G4" shall be read as if it were to "Sections G3.2 to G3.3 and G3.8 to G3.9"; and

(ii) in Section G5.18(b)(iii) to "Sections G5.19 to G5.24" shall be read as if it were to "Section G5.19(d)";

(d) Sections G5.25 and G5.26 (Shared Resources); and

(e) G6 (Anomaly Detection Thresholds: Obligations on the DCC and Users).

Disputes

G1.8 Where, in any dispute between a Party and a User, a question arises as to whether that User has complied with any of its obligations under Sections G3 to G6:

(a) that question may be referred by either of them to the Panel for its determination; and

(b) where either of them disagrees with any such determination of the Panel, then it may refer the matter to the Authority in accordance with Section M7 (Dispute Resolution).

G1.9 Section G1.8:

(a) shall be without prejudice to the provisions of Section M8.2 (Notification of an Event of Default); and

(b) shall not apply in respect of any other question in dispute between a Party and a User relating to or arising from the question of whether the User has complied with any of its obligations under Sections G3 to G6.

SMETS1 Smart Metering Systems

G1.10 Any reference in Sections G2 to G9 to:

(a) a SMETS1 SMS shall be treated as being a reference to an Enrolled SMETS1 SMS only;

(b) a Smart Metering System shall be treated as including a SMETS1 SMS only if it is an Enrolled SMETS1 SMS;

(c) a Device shall be treated as including a SMETS1 Device only if it forms part of or is ancillary to an Enrolled SMETS1 SMS.

The SMETS1 CSP System

G1.11 Section G1.12 applies to the DCC in respect of those parts of the DCC Total System which:

(a) comprise those Systems used by any DCC Service Provider in order to support the provision of Communications Services by the DCC in relation to SMETS1 Devices; and

(b) do not constitute those Systems used by the DCC in its role as a SMETS1 Service Provider or as a DCO that do not also support the provision of Communications Services by the DCC in relation to SMETS2+ Devices,

and, for the purposes of Section G1.12, those parts of the DCC Total System shall be known as the " **SMETS1 CSP System**".

G1.12 Where this Section G1.12 applies, the DCC may comply with its obligations under the provisions listed in Section G1.13 by, in each case, ensuring that the records, processes or procedures described in that provision are, in respect of the SMETS1 CSP System, compliant with:

(a) the standard specified in that provision; or

(b) an alternative standard or methodology that reflects Good Industry Practice in respect of the subject matter of the standard specified in that provision, and that is capable of verification as such by the DCC Independent Security Assurance Service Provider in accordance with Section G9.

G1.13 The provisions listed in this Section G1.13 are the provisions at Sections G2.13, G2.18, G2.26, G2.27, G4.6, G5.7, G5.8 and G5.10.

CSS Provider Systems

G1.14 The security obligations applying to the CSS Provider Systems are set out in Section E2.18 (Security Obligations of the CSS Provider); and

G1.15 In Sections G2 to G9:

(a) other than for the purposes of Section G2.20(a), each and every reference to the DCC Total System shall exclude the CSS Provider Systems; and

(b) each and every reference to the DCC Systems shall exclude the CSS Provider Systems.

G2. SYSTEM SECURITY: OBLIGATIONS ON THE DCC

Unauthorised Activities: Duties to Detect and Respond

G2.1 The DCC shall take reasonable steps:

(a) to ensure that the DCC Systems are capable of detecting any unauthorised connection that has been made to them, and any unauthorised attempt to connect to them, by any other System; and

(b) if the DCC Systems detect such a connection or attempted connection, to ensure that the connection is terminated or the attempted connection prevented (as the case may be).

G2.2 The DCC shall take reasonable steps:

(a) to ensure that the DCC Total System is capable of detecting any unauthorised software that has been installed or executed on it and any unauthorised attempt to install or execute software on it;

(b) if the DCC Total System detects any such software or such attempt to install or execute software, to ensure that the installation or execution of that software is prevented; and

(c) where any such software has been installed or executed, to take appropriate remedial action.

G2.3 The DCC shall:

(a) take reasonable steps to ensure that:

(i) the DCC Total System is capable of identifying any deviation from its expected configuration; and

(ii) any such identified deviation is rectified; and

(b) for these purposes maintain at all times an up-to-date list of all hardware, and of all software and firmware versions and patches, which form part of the configuration of the DCC Total System.

G2.4 The DCC shall take reasonable steps to ensure that the DCC Total System:

(a) is capable of identifying any unauthorised or unnecessary network port, protocol, communication, application or network service;

(b) causes or permits to be open at any time only those network ports, and allows only those protocols, which are required at that time for the effective operation of that System, and blocks all network ports and protocols which are not so required; and

(c) causes or permits at any time only the making of such communications and the provision of such applications and network services as are required at that time for the effective operation of that System.

G2.5 The DCC shall take reasonable steps to ensure that each component of the DCC Total System is, at each point in time, enabled only with the functionality that is necessary for it effectively to fulfil its intended role within the DCC Total System at that time.

G2.6 The DCC shall:

(a) ensure that the DCC Total System records all system activity (including all attempts to access resources, or Data held, on it) in audit logs;

(b) ensure that the DCC Total System detects any attempt by any person to access resources, or Data held, on it without possessing the authorisation required to do so; and

(c) take reasonable steps to ensure that the DCC Total System prevents any such attempt at unauthorised access.

G2.7 The DCC shall take reasonable steps to ensure that the DCC Total System is capable of detecting any instance of Data leaving it by any means (including in particular by network transfers and the use of removable media) without authorisation.

Adverse Events: Duties to Detect and Prevent

G2.8 The DCC shall take reasonable steps to ensure that:

(a) the DCC Total System detects any Denial of Service Event; and

(b) any unused or disabled component or functionality of the DCC Total System is incapable of being a means by which that System is Compromised.

G2.9 The DCC shall use its best endeavours to:

(a) ensure that the DCC Total System is not Compromised;

(b) where the DCC Total System is Compromised, minimise the extent to which it is Compromised and any adverse effect arising from it having been Compromised; and

(c) ensure that the DCC Total System detects any instance in which it has been Compromised.

Security Incident Management

G2.10 The DCC shall ensure that, where the DCC Total System detects any:

(a) unauthorised event or deviation of a type referred to in Sections G2.1 to G2.7; or

(b) event which results, or was capable of resulting, in the DCC Total System being Compromised,

the DCC takes all of the steps required by the DCC Information Security Management System.

G2.11 The DCC shall, on the occurrence of a Major Security Incident in relation to the DCC Total System:

(a) promptly notify the Panel and the Security Sub-Committee (unless paragraph (b) applies); or

(b) where the Major Security Incident relates to that part of the DCC Total System which consists of any parts of the SMETS1 CSP System in respect of which Telefonica UK Limited is the DCC Service Provider, notify the Panel and the Security Sub-Committee as soon as is reasonably practicable.

System Design and Operation

G2.12 G2.12 The DCC shall, at each stage of the System Development Lifecycle, have regard to the need to design and operate the DCC Total System so as to protect it from being Compromised.

Management of Vulnerabilities

G2.13 The DCC shall ensure that an organisation which is a CHECK approved service provider or a CREST certified tester carries out assessments that are designed to identify any vulnerability of the DCC Systems to Compromise:

(a) in respect of each DCC System, on at least an annual basis;

(b) in respect of each new or materially changed component or functionality of the DCC Systems, prior to that component or functionality becoming operational; and

(c) on the occurrence of any Major Security Incident in relation to the DCC Systems.

G2.14 The DCC shall ensure that it carries out assessments that are designed to identify any vulnerability of the DCC Systems to Compromise:

(a) in respect of each DCC System, on at least an annual basis;

(b) in respect of each new or materially changed component or functionality of the DCC Systems, prior to that component or functionality becoming operational; and

(c) on the occurrence of any Major Security Incident in relation to the DCC Systems.

G2.15 Where, following any assessment of the DCC Systems in accordance with Section G2.13 or G2.14, any such vulnerability has been detected, the DCC shall:

(a) take reasonable steps to ensure that the cause of the vulnerability is rectified, or the potential impact of the vulnerability is mitigated, as soon as is reasonably practicable; and

(b) in the case of a material vulnerability, promptly notify the Security Sub- Committee of the steps being taken to rectify its cause or mitigate its potential impact (as the case may be) and the time within which they are intended to be completed.

Management of Data

G2.16 Where the DCC carries out a Back-Up of any Data held on the DCC Total System, it shall ensure that the Data which are Backed-Up are:

(a) protected in accordance with the Information Classification Scheme, including when being transmitted for the purposes of Back-Up; and

(b) stored on media that are located in physically secure facilities, at least one of which facilities must be in a different location to that part of the DCC Total System on which the Data being Backed-Up is ordinarily held.

G2.17 The DCC shall develop and maintain, and hold all Data in accordance with, a DCC Data Retention Policy.

G2.18 The DCC shall ensure that where, in accordance with the DCC Data Retention Policy, any Data are no longer required for the purposes of the Authorised Business, they are securely deleted in compliance with:

(a) HMG Information Assurance Standard No. 5:2011 (Secure Sanitisation); or

(b) any equivalent to that HMG Information Assurance Standard which updates or replaces it from time to time.

DCC Total System: Duty to Separate

G2.19 The DCC shall take reasonable steps to ensure that any software or firmware installed on the DCC Total System for the purposes of security is Separated from any software or firmware that is installed on that System for any other purpose.

G2.20 The DCC shall ensure that:

(a) all DCC Systems which form part of the DCC Total System are Separated from any other Systems;

(b) the DCC IT Testing and Training Systems and DCC IT Supporting Systems are Separated from the DCC Live Systems; and

(c) subject to the provisions of Section G2.22, each DCC Individual Live System is Separated from each other such System.

G2.21 Not used.

G2.22 Any System of the type referred to at paragraph (b) of the definition of DCC Individual Live System in Section A1 (Definitions) need not be Separated from that part of the DCC Total System which is used to convey communications between it and SMETS1 CHs.

DCC Total System: Further provisions for those parts referred to in paragraphs (b) and (c) of the definition of DCC Live Systems

G2.22A The requirements set out in Section G2.22B apply in relation to:

(a) the part of the DCC Total System which is referred to in paragraph (b) of the definition of DCC Live Systems in Section A1 (Definitions); and

(b) the part of the DCC Total System which is referred to in paragraph (c) of the definition of DCC Live Systems in Section A1 (Definitions),

each of which is as a '**relevant system**' for the purposes of Section G2.22B.

G2.22B The DCC shall ensure that:

(a) where a relevant system receives information from, or purporting to be from, the other relevant system, the relevant system receiving the information shall, prior to that information being used by any person, verify that the information:

(i) originated from and was created by the other relevant system; and

(ii) has not been modified since it was created by that relevant system;

(b) it puts in place such additional controls, practices and procedures which (to the extent possible) mitigate the risk of a member of DCC Personnel or a member of personnel of any DCC Service Provider being able to introduce or cause a security vulnerability in a relevant system;

(c) any person engaged in the development or customisation of any bespoke firmware or software relating to a relevant system is not, including for a period of at least 24 months (or such shorter period as may be approved by the Security Sub-Committee) following the date on which they cease to be so engaged on that relevant system, engaged in the development or customisation of bespoke firmware or software relating to the other relevant system;

(d) any person that is authorised as a Privileged Person in relation to a relevant system is not, including for a period of a least six months following the date on which they cease to be authorised as such a Privileged Person for that relevant system, authorised as a Privileged Person in relation to the other relevant system;

(e) any person that is a DCC Service Provider in respect of a relevant system is not a DCC Service Provider in respect of the other relevant system nor an Affiliate or Related Undertaking of any such DCC Service Provider; and

(f) any independent security testing of a relevant system that is used to provide assurance must be carried out by an organisation which is a CHECK approved service provider or a CREST certified tester but is not an organisation that:

(i) designed or developed any relevant system; or

(ii) is an Affiliate or Related Undertaking of an organisation that has designed or developed any relevant system.

DCC Total System: Further provisions for that part referred to in paragraph (c) of the definition of DCC Live Systems

G2.22C The requirements in Sections G2.22D and G2.22E apply in relation to the part of the DCC Total System referred to in paragraph (c) of the definition of DCC Live Systems and referred to in Sections G2.22D and G2.22E the '**applicable system**').

G2.22D The DCC shall ensure that each DCC Service Provider in respect of the applicable system shall, as soon as reasonably practicable, procure, from each company or other person that it knows or should reasonably know is at any time an Ultimate Controller of the DCC Service Provider, a legally enforceable undertaking in favour of the DCC the terms of which provide that the Ultimate Controller will refrain from any action that would be likely to cause the DCC Service Provider to be unable to meet the requirements imposed on it by the DCC for the purposes of enabling the DCC to comply with Section G2.22B(e).

G2.22E The DCC shall ensure that each DCC Service Provider Contract in respect of Services relating to the applicable system shall include terms and conditions which:

(a) require the DCC Service Provider to ensure that it is at all times able to meet the requirements imposed on it by the DCC for the purposes of enabling the DCC to comply with Section G2.22B(e);

(b) provide that where the DCC Service Provider:

(i) fails to procure an undertaking required by the DCC under Section G2.22C; or

(ii) fails to meet the requirements imposed on it by the DCC for the purposes of enabling the DCC to comply with Section G2.22B(e),

the DCC shall be entitled under and in accordance with the DCC Service Provider Contract to:

(iii) require such divestment by the DCC Service Provider as will enable it to meet the requirements imposed on it by the DCC for the purposes of its compliance with Section G2.22B(e);

(iv) terminate the DCC Service Provider Contract in respect of the applicable system and recover from the DCC Service Provider the DCC's costs arising as a direct result of the DCC Service Provider's failure as referred to in Sections G2.22E(b)(i) and (ii), including any fines or re-procurement costs.

Transfer of Secret Key Material

G2.22F Section G2.22G applies where the services provided under any particular DCC Service Provider Contract are (or are to be) replaced (in whole or in part) by the DCC such that they are (or shall be) provided under a different DCC Service Provider Contract.

G2.22G Where this Section G2.22G applies and it is expedient or requisite for the purposes of enabling the DCC to ensure the secure, continued and ongoing provision of services provided by the DCC under the Smart Energy Code, the DCC may, subject to the requirements of Section G2.22I, securely transfer Secret Key Material and other associated information from one DCC Live System or DCC Individual Live System to another DCC Live System or DCC Individual Live System or to a system which is to become part of a DCC Live System or DCC Individual Live System.

G2.22H Where:

(a) a secure transfer of Secret Key Material takes place pursuant to the provisions of Section G2.22G; and

(b) the transferred Secret Key Material includes a Private Key,

any Certificate that contains a Public Key that is associated with that Private Key shall, for the purposes of the Code, be treated as having been issued in respect of the DCC Live System or DCC Individual Live System to which that Secret Key Material has been transferred.

G2.22I The requirements of this Section G2.22I are that where the Secret Key Material relates to, or is used in connection with any Public Key that is the subject of, this Code:

(a) the SMKI PMA has, prior to the transfer of the Secret Key Material or other associated information taking place and having taken account of the views of the Security Sub-Committee on the proposed transfer, approved both:

(i) the secure transfer of that Secret Key Material and any other associated information; and

(ii) the secure mechanism by which the transfer is to take place; and

(b) the DCC ensures that:

(i) the secure transfer of the Secret Key Material and any other associated information is undertaken in compliance with any conditions that maybe specified by the SMKI PMA in its approval (which approval may be given before this Section G2.22I takes effect); and

(ii) the system to which the Secret Key Material and any other associated information is transferred complies with the requirements of Section G,including where that system is to become part of a DCC Live System or a DCC Individual Live System that it complies (to the extent required) with the provisions of Section G that apply or will apply to that DCC Live System or DCC Individual Live System.

DCC Live Systems: Independence of User Systems

G2.23 The DCC shall ensure that no individual is engaged in:

(a) the development of bespoke software or firmware, or the customisation of any software or firmware, for the purpose of its installation on any part of the DCC Live Systems; or

(b) the development, design, build, testing, configuration, implementation, operation, maintenance, modification or decommissioning of any part of the DCC Live Systems,

unless that individual satisfies the requirements of Section G2.24.

G2.24 An individual satisfies the requirements of this Section only if, at any time at which that individual is engaged in any activity described in Section G2.23, he or she:

(a) is not at the same time also engaged in:

(i) the development of bespoke software or firmware, or the customisation of any software or firmware, for the purpose of its installation on any User Systems; or

(ii) the development, design, build, testing, configuration, implementation, operation, maintenance, modification or decommissioning of any User Systems; and

(b) has not been engaged in any activity described in paragraph (a) for a period of time which the DCC reasonably considers to be appropriate, having regard to the need to ensure the management of risk in accordance with the DCC Information Security Management System.

G2.25 The DCC shall ensure that no resources which form part of the DCC Live Systems also form part of any User Systems.

Monitoring and Audit

G2.26 The DCC shall ensure that all system activity audit logs are reviewed regularly in accordance with the DCC Information Security Management System.

G2.27 The DCC shall ensure that all such system activity recorded in audit logs is recorded in a standard format which is compliant with:

(a) British Standard BS 10008:2008 (Evidential Weight and Legal Admissibility of Electronic Information), or any equivalent to that British Standard which updates or replaces it from time to time; and

(b) in the case of activity on the DCC Systems only, the Security Sub-Committee Guidance on Forensic Readiness published on the Website.

G2.28 The DCC shall monitor the DCC Systems in compliance with the SMKI PMA Guidance on Protective Monitoring published on the Website.

G2.29 The DCC shall take reasonable steps to ensure that the DCC Systems are capable of detecting Anomalous Events, in particular by reference to the:

(a) sending or receipt (as the case may be) of Service Requests, Pre-Commands, Signed Pre-Commands, Commands, Instructions to SMETS1 Devices, Service Responses and Alerts;

(b) audit logs of each component of the DCC Total System;

(c) error messages generated by each device which forms part of the DCC Total System;

(d) Incident Management Log compiled in accordance with Section H9; and

(e) patterns of traffic over the SMETS1 SM WAN and the SMETS2+ SM WAN.

G2.30 The DCC shall:

(a) take reasonable steps to ensure that the DCC Systems detect all Anomalous Events; and

(b) ensure that, on the detection of any Anomalous Event, it takes all of the steps required by the DCC Information Security Management System.

Manufacturers: Duty to Notify and Be Notified

G2.31 Where the DCC becomes aware of any material security vulnerability in, or likely cause of a material adverse effect on the security of, any hardware, software or firmware which forms part of the DCC Total System, it shall:

(a) wherever it is reasonably practicable to do so notify the manufacturer of the hardware or the developer of the software or firmware (as the case may be);

(b) take reasonable steps to ensure that the cause of the vulnerability or likely cause of the material adverse effect is rectified, or its potential impact is mitigated, as soon as is reasonably practicable; and

(c) promptly notify the Security Sub-Committee of the steps being taken to rectify the cause of the vulnerability or likely cause of the material adverse effect, or to mitigate its potential impact (as the case may be), and the time within which those steps are intended to be completed.

G2.32 The DCC shall not be required to notify a manufacturer or developer in accordance with Section G2.31(a) where it has reason to be satisfied that the manufacturer or developer is already aware of the matter that would otherwise be notified.

G2.33 The DCC shall, wherever it is reasonably practicable to do so, establish with the manufacturers of the hardware and developers of the software and firmware which form part of the DCC Total System arrangements designed to ensure that the DCC will be notified where any such manufacturer or developer (as the case may be) becomes aware of any material security vulnerability in, or likely cause of a material adverse effect on the security of, such hardware, software or firmware.

G2.34 Any arrangements established in accordance with Section G2.33 may provide that the manufacturer or developer (as the case may be) need not be required to notify the DCC where that manufacturer or developer has reason to be satisfied that the DCC is already aware of the matter that would otherwise be notified under the arrangements.

Parse and Correlate Software: Duty to Notify

G2.35 Where the DCC becomes aware of any material security vulnerability in, or likely cause of a material adverse effect on the security of, any version of the Parse and Correlate Software, it shall notify the Users and (wherever it is reasonably practicable to do so) the developer of the software.

G2.36 The DCC shall not be required to notify a developer or User in accordance with Section G2.35 where it has reason to be satisfied that the developer or User is already aware of the matter that would otherwise be notified.

Cryptographic Credential Tokens and Smart Card Tokens

G2.37 Before supplying any Cryptographic Credential Token or Smart Card Token to any person in accordance with the provisions of this Code, the DCC shall ensure that the version of the software which forms part of that Cryptographic Credential Token or Smart Card Token:

(a) operates so as to generate Public Keys each of which is part of a Key Pair that has been generated using random numbers which are such as to make it computationally infeasible to regenerate that Key Pair even with knowledge of when and by means of what equipment it was generated; and

(b) has been adequately tested for the purpose of ensuring that it fulfils its intended purpose.

G2.38 The DCC shall, wherever it is reasonably practicable to do so, establish with the manufacturers of the hardware and developers of the software and firmware which form part of any Cryptographic Credential Tokens or Smart Card Tokens to be supplied by it in accordance with the provisions of this Code, arrangements designed to ensure that the DCC will be notified where any such manufacturer or developer (as the case may be) becomes aware of any material security vulnerability in, or likely cause of a material adverse effect on the security of, such hardware, software or firmware.

G2.39 Where the DCC becomes aware of any material security vulnerability in, or likely cause of a material adverse effect on the security of, any hardware, software or firmware which form part of any Cryptographic Credential Token or Smart Card Token which has been supplied by it in accordance with the provisions of this Code, it shall notify the Subscribers for Certificates associated with the use of Cryptographic Credential Tokens or Smart Card Tokens and (wherever it is reasonably practicable to do so) the manufacturer of the hardware or (as the case may be) developer of the software or firmware.

File Signing Software

G2.40 Before supplying any File Signing Software to any person in accordance with the provisions of this Code, the DCC shall ensure that the version of that File Signing Software which is being supplied has been subject to a software code review, by an individual or organisation with the professional competence to carry out such a review, for the purpose of identifying any vulnerabilities in the code that were not intended as a feature of its design.

G2.41 The DCC shall, wherever it is reasonably practicable to do so, establish with the developer of the File Signing Software to be supplied by it in accordance with the provisions of this Code, arrangements designed to ensure that the DCC will be notified where that developer becomes aware of any material security vulnerability in, or likely cause of a material adverse effect on the security of, such software.

G2.42 Where the DCC becomes aware of any material security vulnerability in, or likely cause of a material adverse effect on the security of, any File Signing Software which has been supplied by it in accordance with the provisions of this Code, it shall notify each person to whom it has provided that software and (wherever it is reasonably practicable to do so) the developer of the software.

G2.43 The DCC shall ensure that where it provides File Signing Software to any person, that software is provided in a format such that it can be confirmed, on receipt by the person to whom it is provided, as:

(a) having been provided by the DCC; and

(b) being authentic, such that any tampering with the software would be apparent.

Cryptographic Processing

G2.44 The DCC shall ensure that all Cryptographic Processing which:

(a) is for the purposes of complying with its obligations as CoS Party;

(b) results in the application of a Message Authentication Code to any message in order to create a Command to be sent to a SMETS2+ Device;

(c) is carried out by a DCO and involves the use for a SMETS1 Symmetric Key;

(d) involves the use of a DCC Private Key to establish any Transport Layer Security for the purposes of communicating with a SMETS1 Device;

(e) (other than in any of the circumstances set out in Section G2.44A) is carried out by a SMETS1 Service Provider and involves the use of a SMETS1 Symmetric Key; or

(f) (other than in any of the circumstances set out in Section G2.44B) involves the use of a Private Key to create a Digital Signature which is intended to be part of a Command that can be processed by a SMETS2+ Device,

is carried out within Cryptographic Modules which are compliant with FIPS 140-2 Level 3 (or any equivalent to that Federal Information Processing Standard which updates or replaces it from time to time).

G2.44A For the purposes of Section G2.44(e), the circumstances set out in this Section G2.44A shall be those in which one of the following occurs:

(a) Cryptographic Processing is carried out by a SMETS1 Service Provider to generate a Command to "add credit" (as specified in a Version of the ESMETS, the GSMETS or the IHDTS with a Principal Version number of 1) to a SMETS1 Device;

(b) a SMETS1 Symmetric Key is used by a SMETS1 Service Provider to generate an Instruction where the target Device is identified in the SMETS1 Supporting Requirements as a Category 1 Device for the purposes of this paragraph (b);

(c) a SMETS1 Symmetric Key is used by a SMETS1 Service Provider where:

(i) that Symmetric Key is valid only for the duration of a single Application Association; and

(ii) the target Device is identified as a Category 2 Device for the purposes of this sub-paragraph in the SMETS1 Supporting Requirements; and

(d) any use of a SMETS1 Symmetric Key by a SMETS1 Service Provider that is:

(i) required to establish a session for Transport Layer Security with a SMETS1 Device;

(ii) generated as part of the establishment of the session; and

(iii) destroyed at the termination of that same session.

G2.44B For the purposes of Section G2.44(f), the circumstances set out in this Section G2.44B shall be where:

(a) in relation to a Recovery Private Key, there is a period of time during which that Recovery Private Key is unusable for the purposes set out in G2.44 because of it being split into multiple parts as described in Appendix L (SMKI Recovery Procedure); and

(b) in relation to the Contingency Private Key, there is a period of time during which the Contingency Private Key is unusable for the purposes set out in G2.44 because of it being split into multiple parts as described in Appendix L (SMKI Recovery Procedure).

G2.45 The DCC shall ensure that any and all Cryptographic Processing undertaken under or pursuant to this Code which does not fall within the scope of Section G2.44 is carried out within Cryptographic Modules established in accordance with its Information Classification Scheme.

Network Time

G2.46 For the purposes of Section G2.47:

(a) the "**Network Time**" means one or more time sources maintained by the DCC from which all Commissioned Communications Hub Functions synchronise time; and

(b) the "**Independent Time Source**" means a time source that is:

(i) accurate;

(ii) not maintained by the DCC; and

(iii) determined in a manner that is independent of any part of the DCC Total System.

G2.47 The DCC shall ensure that:

(a) the DCC Total System is capable of detecting any instance in which the Network Time materially differs from the Independent Time Source; and

(b) if the DCC Total System detects such a material difference, the DCC takes all of the steps required by the DCC Information Security Management System to rectify the inaccuracy of its Network Time.

Integrity of Communication over the SM WAN

G2.48 The DCC shall take reasonable steps to ensure that all communications which are transmitted over the SM WAN are protected so that the Data contained in them remains confidential, and their integrity is preserved, at all times during transmission to and from Communications Hubs.

G2.49 The DCC shall not process any communication received over the SM WAN, or send to any Party any communication over the SM WAN, where it is aware that the Data contained in that communication has been Compromised.

ECoS Interface Specification

G2.50 The DCC shall, as soon as reasonably practicable after the coming into effect of this Section G2.50, prepare and submit to the Secretary of State for approval an ECoS Interface Specification in accordance with the following process:

(a) the DCC shall send a draft of the ECoS Interface Specification, together with an impact assessment that sets out the DCC's views on any impact that the subject matter of the draft ECoS Interface Specification might reasonably be considered to have on the End-to-End Security Architecture or the risks identified in the Security Risk Assessment (a **Security Impact Assessment**), to the Security Sub-Committee for its review and comments;

(b) having received the Security Sub-Committee's comments and observations on the Security Impact Assessment, the DCC shall as soon as is practicable provide a response to any such comments or observations to the Security Sub-Committee, update the draft ECoS Interface Specification as appropriate to take into account any such comments and observations, and send the updated draft to the Secretary of State, together with:

(i) a statement of the reasons why the DCC considers the submitted draft to be fit for purpose; and

(ii) an explanation of how the DCC has responded to the comments and observations (if any) made by the Security Sub-Committee in respect of the initial draft and/or the Security Impact Assessment sent to it in accordance with paragraph (a) above;

(c) the DCC shall comply with any direction given to it by the Secretary of State following the Secretary of State's consideration of the draft ECoS Interface Specification which direction may require the DCC to:

(i) make such amendments to the draft document as are set out or described in the direction;

(ii) produce and submit to the Secretary of State a further draft of the document; and

(iii) follow a specified process (and the time within which that process shall be completed) prior to submitting a further draft of the document to the Secretary of State.

G2.51 Where pursuant to Section G2.50(b) the Security Sub-Committee receives a response from the DCC in respect of any comments or observations made by the Security Sub-Committee on the Security Impact Assessment, the Security Sub-Committee shall notify the Secretary of State whether it considers there to be any remaining outstanding unacceptable risks to the End-to-End Security Architecture as a consequence of the proposed ECoS Interface Specification.

G2.52 [Not used]

G2.53 Where the DCC wishes to make a change to the ECoS Interface Specification, it shall prepare and submit to the Security Sub-Committee a draft of the proposed amended ECoS Interface Specification, together with an updated Security Impact Assessment that sets out the DCC's views on the impact that the proposed changes might reasonably be considered to have on the End-to-End Security Architecture or the risks identified in the Security Risk Assessment.

G2.54 The DCC shall take into account, and provide a response to, any comments and observations received from the Security Sub Committee when finalising any replacement version of the ECoS Interface Specification.

G2.55 The DCC shall ensure that:

(a) the ECoS Interface Specification accurately describes the ECoS Interface at all times; and

(b) on receiving a request from the DCC Independent Security Assessment Service Provider for the purposes of enabling it to carry out a DCC Security Assessment, the ECoS Interface Specification is made available to the DCC Independent Security Assessment Service Provider together with all previous versions of the specification and any supporting Security Impact Assessments as may be requested by the DCC Independent Security Assessment Service Provider.

DCC Use of Private Keys

G2.56 The DCC shall ensure that any Private Key that it uses or intends to use to create a Digital Signature that forms part of a Command that is to be sent to a SMETS2+ Device is used only for the purposes of:

(a) creating Digital Signatures that form part of Commands that are to be sent to SMETS2+ Devices; or

(b) Digitally Signing Certificate Signing Requests.

G2.57 Where:

(a) the DCC is the Subscriber for an Organisation Certificate that has a Remote Party Role that is specified in the GB Companion Specification; and

(b) the Private Key associated with the Public Key contained within that Organisation Certificate is used for purposes that are not specified or described in the GB Companion Specification,

the DCC shall, where reasonably possible at the earliest opportunity but in any event no later than the date of expiry of that Organisation Certificate, replace the Private Key with one that has an associated Public Key that is contained within an Organisation Certificate that has a Remote Party Role that is specified in Table 1 to Annex A of Section L.

G2.58 Subject to Section G2.59, the DCC shall not, on or from a date which is after the ECoS Service Live Date, become a Subscriber for an Organisation Certificate that:

(a) has a Remote Party Role that is specified in the GB Companion Specification; and

(b) contains a Public Key which has an associated Private Key that is used, or is to be used, for purposes that are not specified or described in the GB Companion Specification.

G2.59 The requirement in Section G2.58 shall not apply in circumstances where the DCC is required to replace an Organisation Certificate that has:

(a) a Remote Party Role that is specified in the GB Companion Specification; and

(b) been revoked following the operation of one of the procedures in the SMKI Recovery Procedure.

G2.60 The DCC shall ensure that any Root OCA Private Key is used only for the purposes of:

(a) Digitally Signing an OCA Certificate;

(b) Digitally Signing a Certificate Signing Request; or

(c) Digitally Signing the Organisation ARL.

G2.61 The DCC shall ensure that any Issuing OCA Private Key is used only for the purposes of:

(a) Digitally Signing an Organisation Certificate;

(b) Digitally Signing a Certificate Signing Request; or

(c) Digitally Signing the Organisation CRL.

G3. SYSTEM SECURITY: OBLIGATIONS ON USERS

Unauthorised Activities: Duties to Detect and Respond

G3.1 Each User shall:

(a) take reasonable steps to ensure that:

(i) its User Systems are capable of identifying any deviation from their expected configuration; and

(ii) any such identified deviation is rectified; and

(b) for these purposes maintain at all times an up-to-date list of all hardware, and of all software and firmware versions and patches, which form part of the configuration of those User Systems.

G3.2 Each User shall take reasonable steps:

(a) to ensure that its User Systems are capable of detecting any unauthorised software that has been installed or executed on them and any unauthorised attempt to install or execute software on them;

(b) if those User Systems detect any such software or such attempt to install or execute software, to ensure that the installation or execution of that software is prevented; and

(c) where any such software has been installed or executed, to take appropriate remedial action.

G3.3 Each User shall:

(a) ensure that its User Systems record all attempts to access resources, or Data held, on them;

(b) ensure that its User Systems detect any attempt by any person to access resources, or Data held, on them without possessing the authorisation required to do so; and

(c) take reasonable steps to ensure that its User Systems prevent any such attempt at unauthorised access.

Security Incident Management

G3.4 Each User shall ensure that, on the detection of any unauthorised event of the type referred to at Sections G3.1 to G3.3, it takes all of the steps required by its User Information Security Management System.

G3.5 Each User shall, on the occurrence of a Major Security Incident in relation to its User Systems, ensure that the Panel and the Security Sub-Committee are promptly notified.

System Design and Operation

G3.6 Each User shall, at each stage of the System Development Lifecycle, have regard to the need to design and operate its User Systems so as to protect them from being Compromised.

Management of Vulnerabilities

G3.7 Each Supplier Party shall ensure that either a tester who has achieved CREST certification or an organisation which is a CHECK service provider carries out assessments that are designed to identify any vulnerability of its User Systems to Compromise:

(a) in respect of each of its User Systems, on at least an annual basis;

(b) in respect of each new or materially changed component or functionality of its User Systems, prior to that component or functionality becoming operational; and

(c) on the occurrence of any Major Security Incident in relation to its User Systems.

G3.8 Each User shall ensure that it carries out assessments that are designed to identify any vulnerability of its User Systems to Compromise:

(a) in respect of each of its User Systems, on at least an annual basis;

(b) in respect of each new or materially changed component or functionality of its User Systems, prior to that component or functionality becoming operational; and

(c) on the occurrence of any Major Security Incident in relation to its User Systems.

G3.9 Each User shall ensure that:

(a) in respect of any new or materially changed component or functionality of its User Systems which comprises (or includes) a System that is being incorporated into its User Systems for the first time:

(i) it notifies the Security Sub-Committee prior to that System becoming an operational part of its User Systems;

(ii) together with that notification it provides to the Security Sub-Committee an adequate description of the System, of the purpose for which it will be used, and of the nature of its relationship to the other component parts of the User Systems; and

(iii) that System does not become an operational part of its User Systems unless and until the Security Sub-Committee has authorised the User to bring it into operation (for which purpose, following any such review or assessment as it may consider appropriate, the Security Sub-

Committee shall be entitled to give or withhold authorisation by means of notice to the User); and

(b) where, following any assessment of its User Systems in accordance with Section G3.7 or G3.8, any material vulnerability has been detected, a User shall ensure that it:

(i) takes reasonable steps to ensure that the cause of the vulnerability is rectified, or the potential impact of the vulnerability is mitigated, as soon as is reasonably practicable;

(ii) promptly notifies the Security Sub-Committee of the steps being taken to rectify its cause or mitigate its potential impact (as the case may be) and the time within which they are intended to be completed; and

(c) where a material component or material functionality of its User Systems is being discontinued or where a User System is being decommissioned;

(i) the User notifies the Security Sub-Committee prior to the component or functionality being discontinued or the User System being decommissioned (as relevant);

(ii) together with that notification, the User provides to the Security Sub-Committee an adequate description of the reason for the change and the proposed timing of the change;

(iii) the discontinuation or decommissioning is not undertaken before the Security Sub-Committee has been notified; and

(iv) the User takes any reasonable action advised by the Security Sub-Committee.

Management of Data

G3.10 Each User shall:

(a) develop and maintain, and hold all Data in accordance with, a User Data Retention Policy; and

(b) when any Data held by it cease to be retained in accordance with the User Data Retention Policy, ensure that they are securely deleted in accordance with its Information Classification Scheme.

User Systems: Duty to Separate

G3.11 Each User shall take reasonable steps to ensure that any software or firmware that is installed on its User Systems for the purposes of security is Separated from any software or firmware that is installed on those Systems for any other purpose.

User Systems: Independence of DCC Live Systems

G3.12 Each User shall ensure that no individual is engaged in:

(a) the development of bespoke software or firmware, or the customisation of any software or firmware, for the purpose of its installation on any part of its User Systems; or

(b) the development, design, build, testing, configuration, implementation, operation, maintenance, modification or decommissioning of any part of its User Systems, unless that individual satisfies the requirements of Section G3.13.

G3.13 An individual satisfies the requirements of this Section only if, at any time at which that individual is engaged in any activity described in Section G3.12, he or she:

(a) is not at the same time also engaged in:

(i) the development of bespoke software or firmware, or the customisation of any software or firmware, for the purpose of its installation on any part of the DCC Live Systems; or

(ii) the development, design, build, testing, configuration, implementation, operation, maintenance, modification or decommissioning of any part of the DCC Live Systems; and

(b) has not been engaged in any activity described in paragraph (a) for a period of time which the User reasonably considers to be appropriate, having regard to the need to ensure the management of risk in accordance with its User Information Security Management System.

G3.14 Each User shall ensure that no resources which form part of its User Systems also form part of the DCC Live Systems.

Monitoring

G3.15 Each Supplier Party shall take reasonable steps to ensure that its User Systems are capable of detecting Anomalous Events, in particular by reference to the:

(a) sending or receipt (as the case may be) of Service Requests, Pre-Commands, Signed Pre-Commands, Service Responses and Alerts;

(b) audit logs of each Device for which it is the Responsible Supplier; and

(c) error messages generated by each Device for which it is the Responsible Supplier.

G3.16 Each Supplier Party shall:

(a) take reasonable steps to ensure that its User Systems detect all Anomalous Events; and

(b) ensure that, on the detection by its User Systems of any Anomalous Event, it takes all of the steps required by its User Information Security Management System.

Manufacturers: Duty to Notify and Be Notified

G3.17 Where a User becomes aware of any material security vulnerability in, or likely cause of a material adverse effect on the security of:

(a) any hardware, software or firmware which forms part of its User Systems; or

(b) (where applicable) any Smart Metering System (excluding a Communications Hub Function or Gas Proxy Function which forms part of a SMETS2+ Device) for which it is the Responsible Supplier,

it shall comply with the requirements of Section G3.18.

G3.18 The requirements of this Section are that the User shall:

(a) wherever it is reasonably practicable to do so notify the manufacturer of the hardware or Device or the developer of the software or firmware (as the case may be);

(b) take reasonable steps to ensure that the cause of the vulnerability or likely cause of the material adverse effect is rectified, or its potential impact is mitigated, as soon as is reasonably practicable; and

(c) ensure that the Security Sub-Committee is promptly notified of the steps being taken to rectify the cause of the vulnerability or likely cause of the material adverse effect, or to mitigate its potential impact (as the case may be), and the time within which those steps are intended to be completed.

G3.19 A User shall not be required to notify a manufacturer or developer in accordance with Section G3.18(a) where it has reason to be satisfied that the manufacturer or developer is already aware of the matter that would otherwise be notified.

G3.20 Each User shall, wherever it is practicable to do so, establish with:

(a) the manufacturers of the hardware and developers of the software and firmware which form part of its User Systems; and

(b) (where applicable) any Smart Metering System (excluding a Communications Hub Function or Gas Proxy Function which forms part of a SMETS2+ Device) for which it is the Responsible Supplier,

arrangements designed to ensure that the User will be notified where any such manufacturer or developer (as the case may be) becomes aware of any material security vulnerability in, or likely cause of a material adverse effect on the security of, such hardware, software, firmware or Device.

G3.21 Any arrangements established in accordance with Section G3.20 may provide that the manufacturer or developer (as the case may be) need not be required to notify the User where that manufacturer or developer has reason to be satisfied that the User is already aware of the matter that would otherwise be notified under the arrangements.

Cryptographic Processing

G3.22 Each User shall ensure that it carries out Cryptographic Processing only within Cryptographic Modules established in accordance with its Information Classification Scheme.

User Systems: Physical Location

G3.23 Each User which is an Eligible User in relation to any Supply Sensitive Service Request shall ensure that:

(a) any Cryptographic Module which constitutes a component of its User Systems and in which:

(i) any Private Key that is used to Digitally Sign Pre-Commands is held;

(ii) Pre-Commands are Digitally Signed; and

(iii) any SMETS1 Service Request that constitutes a Critical Service Request is Digitally Signed; and

(b) any functionality of its User Systems which is used to apply Supply Sensitive Checks, is located, operated, configured, tested and maintained in the United Kingdom by User Personnel who are located in the United Kingdom.

G3.24 Each User to which Section G3.23 applies shall ensure that the components and the functionality of its User Systems to which that Section refers are operated from a sufficiently secure environment in accordance with the provisions of Section G5.17.

Supply Sensitive Check

G3.25 Each User which is an Eligible User in relation to any Supply Sensitive Service Request shall ensure that:

(a) it applies a Supply Sensitive Check prior to Digitally Signing a Pre-Command or SMETS1 Service Request in respect of any Supply Sensitive Service Request;

(b) it both applies that Supply Sensitive Check and Digitally Signs the relevant Pre-Command or SMETS1 Service Request in the United Kingdom; and

(c) the relevant Pre-Command or SMETS1 Service Request has been processed only in the United Kingdom between the application of the Supply Sensitive Check and the Digital Signature.

SMETS1 Smart Metering Systems

G3.26 Each Supplier Party shall use its best endeavours to ensure that each SMETS1 SMS for which it is the Responsible Supplier is at all times Secure.

G3.27 Each Supplier Party shall retain documentary evidence sufficient to demonstrate its compliance with the obligation at Section G3.26.

G3.28 For the purposes of Section G3.26:

(a) a SMETS1 SMS is "**Secure**" if it is designed, installed, operated and supported so as to ensure, to an Appropriate Standard, that it is not subject to any event which results, or is capable of resulting, in any Device of which it is comprised being Compromised to a material extent; and

(b) an "**Appropriate Standard**" means a high level of security that is in accordance with good industry practice within the energy industry in Great Britain, and is capable of verification as such by the User Independent Security Assurance Service Provider in accordance with Section G8.

User Use of Private Keys

G3.29 Each User shall ensure that any Private Key that it uses or intends to use to create a Digital Signature that forms part of a Command that is to be sent to a SMETS2+ Device is used only for the purposes of:

(a) creating Digital Signatures that form part of Commands that are to be sent to SMETS2+ Devices; or

(b) Digitally Signing Certificate Signing Requests.

G4. ORGANISATIONAL SECURITY: OBLIGATIONS ON USERS AND THE DCC

Obligations on Users

G4.1 Each User shall:

(a) ensure that each member of its User Personnel who is authorised to access Data held on its User Systems holds a security clearance which is appropriate to the role performed by that individual and to the Data which he or she is authorised to access; and

(b) annually review the security clearance held by each such individual and ensure that it continues to be appropriate to the role performed by that individual and to the Data which he or she is authorised to access.

G4.2 Each User shall comply with Section G4.3 in respect of any of its User Personnel who are authorised to carry out activities which:

(a) involve access to resources, or Data held, on its User Systems; and

(b) are capable of Compromising the DCC Total System, any User Systems, any RDP Systems or any Device in a manner that could affect (either directly or indirectly) the quantity of gas or electricity that is supplied to a consumer at premises.

G4.3 Each User shall ensure that any of its User Personnel who are authorised to carry out the activities identified in Section G4.2:

(a) where they are located in the United Kingdom are subject to security screening in a manner that is compliant with:

(i) British Standard BS 7858:2012 (Security Screening of Individuals Employed in a Security Environment – Code of Practice); or

(ii) any equivalent to that British Standard which updates or replaces it from time to time; and

(b) where they are not located in the United Kingdom are subject to security screening in a manner that is compliant with:

(i) the British Standard referred to in Section G4.3(a); or

(ii) any comparable national standard applying in the jurisdiction in which they are located.

Obligations on the DCC

G4.4 The DCC shall:

(a) ensure that each member of DCC Personnel who is authorised to access Data held on the DCC Total System holds a security clearance which is appropriate to the role performed by that individual and to the Data to which he or she is authorised to access; and

(b) annually review the security clearance held by each such individual and ensure that it continues to be appropriate to the role performed by that individual and to the Data to which he or she is authorised to access.

G4.5 The DCC shall comply with Section G4.6 in respect of any of the DCC Personnel who are authorised to carry out activities which:

(a) involve access to resources, or Data held, on the DCC Total System; and

(b) are capable of Compromising the DCC Total System, any User Systems, any RDP Systems or any Device.

G4.6 The DCC shall ensure that any of the DCC Personnel who are authorised to carry out the activities identified in Section G4.5:

(a) where they are located in the United Kingdom are subject to security screening in a manner that is compliant with:

(i) British Standard BS 7858:2012 (Security Screening of Individuals Employed in a Security Environment – Code of Practice); or

(ii) any equivalent to that British Standard which updates or replaces it from time to time; and

(b) where they are not located in the United Kingdom are subject to security screening in a manner that is compliant with:

(i) the British Standard referred to in Section G4.6(a); or

(ii) any comparable national standard applying in the jurisdiction in which they are located.

G4.7 The DCC shall ensure that each member of DCC Personnel who is a Privileged Person has passed a Security Check before being given any access to Data held on the DCC Total System.

G4.8 Where the DCC is required to ensure that any two Systems forming part of the DCC Total System are Separated, it shall either:

(a) ensure that no person is a Privileged Person in relation to both of those Systems; or

(b) to the extent that any person is a Privileged Person in relation to both Systems, it establishes additional controls sufficient to ensure that the activities of that person cannot become a means by which any part of the DCC Live Systems is Compromised to a material extent.

G5. INFORMATION SECURITY: OBLIGATIONS ON THE DCC AND USERS

Information Security: Obligations on the DCC

G5.1 The DCC shall establish, maintain and implement processes for the identification and management of the risk of Compromise to the DCC Total System, and such processes shall comply with:

(a) the standard of the International Organisation for Standards in respect of information security risk management known as ISO/IEC 27005:2011 (Information Technology – Security Techniques – Information Security Risk Management); or

(b) any equivalent to that standard of the International Organisation for Standards which updates or replaces it from time to time

G5.2 The DCC shall carry out an assessment of such processes for the identification and management of risk:

(a) on at least an annual basis;

(b) on any occasion on which it implements a material change to the DCC Total System; and

(c) on the occurrence of any Major Security Incident in relation to the DCC Total System.

G5.3 Where the DCC is required in accordance with the DCC Licence to obtain and hold ISO 27001 certification, it shall:

(a) establish, give effect to, maintain, and comply with a set of policies and procedures to be known as the DCC Information Security Management System;

(b) ensure that the DCC Information Security Management System:

(i) is so designed as to ensure that the DCC complies with its obligations under Sections G2 and G4;

(ii) meets the requirements of Sections G5.4 to G5.13; and

(iii) provides for security controls which are proportionate to the potential impact of each part of the DCC Total System being Compromised, as determined by means of processes for the management of information risk; and

(c) review the DCC Information Security Management System on at least an annual basis, and make any changes to it following such a review in order to ensure that it remains fit for purpose.

The DCC Information Security Management System

G5.4 The DCC Information Security Management System shall incorporate an information security policy which makes appropriate provision in respect of:

(a) measures to identify and mitigate risks to the security of Data stored on or communicated by means of the DCC Total System, including measures relating to Data handling, retention and protection; and

(b) the establishment and maintenance of an Information Classification Scheme in relation to the DCC Total System.

G5.5 The DCC Information Security Management System shall specify the approach of the DCC to:

(a) information security, including its arrangements to review that approach at planned intervals;

(b) human resources security;

(c) physical and environmental security; and

(d) ensuring that the DCC Service Providers establish and maintain information, human resources, and physical and environmental security measures which are equivalent to those of the DCC.

G5.6 The DCC Information Security Management System shall incorporate a set of asset management procedures which shall make provision for the DCC to establish and maintain a register of the physical and information assets on which it relies for the purposes of the Authorised Business (including a record of the member of DCC Personnel who has responsibility for each such asset).

G5.7 The DCC Information Security Management System shall incorporate procedures that comply with:

(a) 2021 Telecommunications (Security) Act (TSA) in respect of the security of telecommunications systems and services; or

(b) any equivalent to those Security Procedures which update or replace them from time to time.

G5.8 The DCC Information Security Management System shall incorporate procedures that comply with:

(a) the appropriate standards of the International Organisation for Standards with respect to network security, comprising ISO/IEC 27033-1:2009, ISO/IEC 27033-2:2012 and ISO/IEC 27033-3:2010 (Information Technology – Security Techniques – Network Security); or

(b) any equivalents to those standards of the International Organisation for Standards which update or replace them from time to time.

G5.9 The DCC Information Security Management System shall incorporate a policy on access control, which includes provision in respect of:

(a) measures to restrict access to Data that is stored on or communicated by means of the DCC Total System to those who require such Data and are authorised to obtain it;

(b) the designation of appropriate levels of identity assurance in respect of those who are authorised to access such Data;

(c) the specification of appropriate levels of security clearance in respect of those who are authorised to access such Data;

(d) procedures for granting, amending and removing authorisations in respect of access to such Data;

(e) procedures for granting and reviewing security clearances for DCC Personnel; and

(f) measures to ensure that the activities of one individual may not become a means by which the DCC Total System is Compromised to a material extent.

G5.10 The DCC Information Security Management System shall incorporate procedures on the management of information security incidents which comply with:

(a) the standard of the International Organisation for Standards in respect of security incident management known as ISO/IEC 27035:2011 (Information Technology – Security Techniques – Information Security Incident Management); or

(b) any equivalent to that standard of the International Organisation for Standards which updates or replaces it from time to time.

G5.11 The DCC Information Security Management System shall incorporate procedures on the management of information security incidents which in particular make provision for:

(a) the allocation of clearly defined roles and responsibilities to DCC Personnel;

(b) the manner in which such incidents will be monitored, classified, reported and managed;

(c) a communications plan in relation to all communications with respect to such incidents; and

(d) the use of recovery systems in the case of serious incidents.

G5.12 The DCC Information Security Management System shall incorporate procedures on the management of business continuity that comply with:

(a) the following standards of the International Organisation for Standards in respect of business continuity:

(i) ISO/IEC 22301:2012 (Societal Security – Business Continuity Management Systems – Requirements); and

(ii) ISO/IEC 27031:2011 (Information Technology – Security Techniques – Guidelines for Information and Communications Technology Readiness for Business Continuity); and

(b) the Business Continuity Institute Good Practice Guidelines 2013; or

(c) in each case, any equivalents to those standards or guidelines which update or replace them from time to time.

G5.13 The DCC Information Security Management System shall incorporate procedures in relation to the secure management of all Secret Key Material of the DCC, which shall in particular make provision for:

(a) the security of that Secret Key Material throughout the whole of its lifecycle from its generation to its destruction;

(b) the manner in which that Secret Key Material will be registered, ordered, generated, labelled, distributed, installed, superseded and renewed; and

(c) the verifiable destruction of that Secret Key Material.

Information Security: Obligations on Users

G5.14 Each User shall establish, maintain and implement processes for the identification and management of the risk of Compromise to:

(a) its User Systems;

(b) any security functionality used for the purposes of complying with the requirements of this Section G in relation to its User Systems;

(c) any other Data, Systems or processes on which it relies for the generation, initiation or processing of Service Requests, Service Responses, Alerts or Data communicated over the Self-Service Interface;

(d) any Smart Metering Systems for which it is the Responsible Supplier; and

(e) any communications links established between any of its Systems and the DCC Total System, and any security functionality used in respect of those communications links or the communications made over them.

G5.15 Each User shall ensure that such processes for the identification and management of risk comply with:

(a) the standard of the International Organisation for Standards in respect of information security risk management known as ISO/IEC 27005:2011 (Information Technology – Security Techniques – Information Security Risk Management); or

(b) any equivalent to that standard of the International Organisation for Standards which updates or replaces it from time to time.

G5.16 Each User shall carry out an assessment of such processes for the identification and management of risk:

(a) on at least an annual basis;

(b) on any occasion on which it implements a material change to:

(i) its User Systems;

(ii) any security functionality used for the purposes of complying with the requirements of this Section G in relation to its User Systems;

(iii) any other Systems or processes on which it relies for the generation, initiation or processing of Service Requests, Service Responses, Alerts or Data communicated over the Self-Service Interface; or

(iv) any Smart Metering Systems for which it is the Responsible Supplier; and

(c) on the occurrence of any Major Security Incident in relation to its User Systems.

G5.17 Each User shall comply with the following standard of the International Organisation for Standards in respect of the security, reliability and resilience of its information assets and processes and its User Systems:

(a) ISO/IEC 27001:2013 (Information Technology – Security Techniques – Information Security Management Systems); or

(b) any equivalent to that standard which updates or replaces it from time to time.

G5.18 Each User shall:

(a) establish, give effect to, maintain, and comply with a set of policies and procedures to be known as its User Information Security Management System;

(b) ensure that its User Information Security Management System:

(i) is so designed as to ensure that it complies with its obligations under Sections G3 and G4;

(ii) is compliant with the standard referred to at Section G5.17;

(iii) meets the requirements of Sections G5.19 to G5.24; and

(iv) provides for security controls which are proportionate to the potential impact of each part of its User Systems being Compromised, as determined by means of processes for the management of information risk; and

(c) review its User Information Security Management System on at least an annual basis, and make any changes to it following such a review in order to ensure that it remains fit for purpose.

The User Information Security Management System

G5.19 Each User Information Security Management System shall incorporate an information security policy which makes appropriate provision in respect of:

(a) measures to identify and mitigate risks to the security of Data stored on or communicated by means of the User Systems, including measures relating to Data handling, retention and protection;

(b) the establishment and maintenance of an Information Classification Scheme in relation to the User Systems;

(c) the management of business continuity; and

(d) the education, training and awareness of User Personnel in relation to information security.

G5.20 Each User Information Security Management System shall specify the approach of the User to:

(a) information security, including its arrangements to review that approach at planned intervals;

(b) human resources security;

(c) physical and environmental security; and

(d) ensuring that any person who provides services to the User for the purpose of ensuring that the User is able to comply with its obligations under this Code must establish and maintain information, human resources, and physical and environmental security measures which are equivalent to those of the User.

G5.21 Each User Information Security Management System shall incorporate a set of asset management procedures which shall make provision for the User to establish and maintain a register of the physical and information assets on which it relies for the purposes of complying with its obligations under this Code.

G5.22 Each User Information Security Management System shall incorporate a policy on access control, which includes provision in respect of:

(a) measures to restrict access to Data that is stored on or communicated by means of the User Systems to those who require such Data and are authorised to obtain it;

(b) procedures for granting, amending and removing authorisations in respect of access to such Data; and

(c) measures to ensure that the activities of one individual may not become a means by which the User Systems are Compromised to a material extent.

G5.23 Each User Information Security Management System shall incorporate procedures on the management of information security incidents which comply with:

(a) the standard of the International Organisation for Standards in respect of security incident management known as ISO/IEC 27035:2011 (Information Technology – Security Techniques – Information Security Incident Management); or

(b) any equivalent to that standard of the International Organisation for Standards which updates or replaces it from time to time.

G5.24 Each User Information Security Management System shall incorporate procedures in relation to the secure management of all Secret Key Material of the User, which shall in particular make provision for:

(a) the security of that Secret Key Material throughout the whole of its lifecycle from its generation to its destruction;

(b) the manner in which that Secret Key Material will be registered, ordered, generated, labelled, distributed, installed, superseded and renewed; and

(c) the verifiable destruction of that Secret Key Material.

Shared Resources

G5.25 Sections G5.26 to G5.28 apply in relation to a User where:

(a) any resources which form part of the User Systems of that User (are **Shared Resources**); and

(b) by virtue of those Shared Resources:

(i) the User Systems of that User are capable of being a means by which the User Systems of another User are Compromised (or vice versa); or

(ii) the potential extent to which the User Systems of either User may be Compromised, or the potential adverse effect of any Compromise to the User Systems of either User, is greater than it would have been had those User Systems not employed the Shared Resources.

G5.26 Where this Section applies, a User which begins to employ User Systems which consist in whole or in part of Shared Resources:

(a) shall notify the Security Sub-Committee as soon as reasonably practicable after first doing so; and

(b) where those Shared Resources are provided to the User by a Shared Resource Provider, shall include in that notification:

(i) the name and contact details of the Shared Resource Provider; and

(ii) a description of the services provided by the Shared Resource Provider to the User in relation to its User Systems.

G5.27 Where this Section applies, and where a User is entitled to send Critical Service Requests to the DCC, the User shall notify the Security Sub-Committee of the total number of Smart Metering Systems comprising Devices in respect of which such Critical Service Requests are capable of being sent from its User Systems:

(a) as soon as reasonably practicable after it first begins to employ User Systems which consist in whole or in part of Shared Resources; and

(b) at intervals of six months thereafter.

G5.28 Where this Section applies:

(a) the requirement at Section G5.18(b)(iv) shall be read as a requirement on a User to ensure that its User Information Security Management System provides for security controls that are proportionate to the potential impact of a Compromise to each part of all of the User Systems of each User which employs the Shared Resources; and

(b) where the Shared Resources are provided to a User by a Shared Resource Provider:

(i) the provisions of paragraph (a) apply to the Shared Resource Provider in respect of its own User Information Security Management System in the same manner as they apply to each User to which the Shared Resources are provided; and

(ii) both the User and the Shared Resource Provider shall ensure that their User Information Security Management Systems are compatible with each other in respect of all the matters referred to in Sections G5.19 to G5.24.

G6. ANOMALY DETECTION THRESHOLDS: OBLIGATIONS ON THE DCC AND USERS

Threshold Anomaly Detection Procedures

G6.1 The "**Threshold Anomaly Detection Procedures**" shall be a SEC Subsidiary Document of that name which:

(a) shall describe the means by which:

(i) each User shall be able securely to notify the DCC of the Anomaly Detection Thresholds set by that User, and of any exceptions that are applicable to each such Anomaly Detection Threshold;

(ii) the DCC shall be able securely to notify each User when a communication relating to that User is quarantined, or deleted from the DCC Systems, by the DCC; and

(iii) each such User shall be able securely to notify the DCC whether it considers that a communication which has been quarantined should be deleted from the DCC Systems or processed by the DCC;

(b) shall determine the standard of security at which Users and the DCC must be able to notify each other in order for such notifications to be considered, for the purposes of paragraph (a), to have been given 'securely';

(c) may make provision relating to the setting by Users and the DCC of Anomaly Detection Thresholds, including the issue of guidance by the DCC in relation to the appropriate level at which Anomaly Detection Thresholds should be set by Users; and

(d) may make provision relating to the actions to be taken by Users and the DCC in cases in which an Anomaly Detection Threshold has been exceeded, which:

(i) in the case of any SMETS1 Service Request which contains a data value that is inconsistent with a maximum or minimum set in accordance with paragraph (b)(ii) of the definition of Anomaly Detection Threshold in Section A1 (Definitions), shall include the deletion by the DCC of that Service Request and notification of the User that the deletion has taken place; and

(ii) in any other case, may include provision for communications to be quarantined and remedial action to be taken.

Anomaly Detection Thresholds: Obligations on Users

G6.2 Each User shall comply with any requirements of the Threshold Anomaly Detection Procedures which are applicable to it.

G6.3 Each User which is an Eligible User in relation to any one or more individual Services listed in the DCC User Interface Services Schedule:

(a) shall, in respect of each User ID used by it in any User Role by virtue of which it is such an Eligible User, set Anomaly Detection Thresholds in respect of:

(i) the sum total of the number of Critical Commands and the number of SMETS1 Service Requests that are Critical Service Requests which relate to each such Service Reference Variant; and

(ii) the total number of Service Requests relating to each such Service Reference Variant in respect of which, if the relevant Device were a SMETS2+ Device, there are Service Responses that would contain Data of a type which is Encrypted in accordance with the GB Companion Specification; and

(b) may, at its discretion, set other Anomaly Detection Thresholds.

G6.4 Where a User sets any Anomaly Detection Threshold in accordance with Section G6.3, it shall:

(a) set that Anomaly Detection Threshold at a level designed to ensure that it will function, when used for the purposes of Threshold Anomaly Detection, as an effective means of detecting any Compromise to any relevant part of its User Systems;

(b) before doing so, take into account any guidance issued by the DCC as to the appropriate level of the Anomaly Detection Threshold; and

(c) after doing so, notify the DCC of that Anomaly Detection Threshold.

G6.4A Where, in accordance with the Common Test Scenarios Document, a User becomes an Eligible User for a User Role without successfully completing testing for a Critical Service Request which can potentially be sent by a User in that User Role, then the User must set an Anomaly Detection Threshold of zero in respect of that Critical Service Request.

Anomaly Detection Thresholds: Obligations on the DCC

G6.5 The DCC shall comply with any requirements of the Threshold Anomaly Detection Procedures which are applicable to it.

G6.6 The DCC:

(a) shall, for each individual Service Reference Variant listed in the DCC User Interface Services Schedule, set an Anomaly Detection Threshold in respect of:

(i) the sum total of the number of Critical Commands and the number of SMETS1 Service Requests that are Critical Service Requests which relate to that Service Reference Variant; and

(ii) the total number of Service Requests relating to that Service Reference Variant in respect of which, if the relevant Device were a SMETS2+ Device, there would be Service Responses containing Data of a type which is Encrypted in accordance with the GB Companion Specification;

(b) shall set an Anomaly Detection Threshold in respect of a data value that has been agreed with the Security Sub-Committee within each Signed Pre- Command relating to that Service Reference Variant and SMETS1 Service Request;

(c) shall set an Anomaly Detection Threshold in respect of the total number of each type of Critical Command that is not related to a Service Reference Variant listed in Appendix E (the DCC User Interface Services Schedule); and

(d) may, at its discretion, set other Anomaly Detection Thresholds.

G6.6A The DCC shall, from no later than the ECoS Service Live Date, ensure that where an amended Anomaly Detection Threshold is notified in respect of any part of the DCC Live Systems, that amended Anomaly Detection Threshold shall only be applied in respect of that part of the DCC Live Systems following:

(a) a successful Check Cryptographic Protection of the communication providing the notification of the amended Anomaly Detection Threshold in respect of that part of the DCC Live Systems; and

(b) confirmation that the communication providing the notification of the amended Anomaly Detection Threshold has not previously been the subject of a successful Check Cryptographic Protection in respect of that part of the DCC Live Systems.

G6.7 Where the DCC sets any Anomaly Detection Threshold in accordance with Section G6.6, it shall:

(a) set that Anomaly Detection Threshold at a level designed to ensure that it will function, when used for the purposes of Threshold Anomaly Detection, as an effective means of detecting any Compromise to any relevant part of the DCC Total System or of any User Systems; and

(b) before doing so consult, and take into account the opinion of, the Security Sub- Committee as to the appropriate level of the Anomaly Detection Threshold.

G6.8 The DCC shall notify the Security Sub-Committee of:

(a) each Anomaly Detection Threshold that it sets; and

(b) each Anomaly Detection Threshold that is set by a User and notified to the DCC in accordance with Section G6.4(c).

G6.9 Where the DCC is consulted by a User in relation to an Anomaly Detection Threshold which that User proposes to set, the DCC shall:

(a) provide to the User its opinion as to the appropriate level of that Anomaly Detection Threshold; and

(b) in doing so, have regard to the need to ensure that it will function, when used for the purposes of Threshold Anomaly Detection, as an effective means of detecting any Compromise to any relevant part of the User Systems of that User.

Anomaly Detection Thresholds: Obligations on the DCC and Users

G6.10 The DCC and each User shall, in relation to each Anomaly Detection Threshold that it sets:

(a) keep the Anomaly Detection Threshold under review, having regard to the need to ensure that it continues to function, when used for the purposes of Threshold Anomaly Detection, as an effective means of detecting any Compromise to any relevant part of the DCC Total System and/or User Systems (as the case may be);

(b) for this purpose have regard to any opinion provided to it by the Security Sub- Committee from time to time as to the appropriate level of the Anomaly Detection Threshold; and

(c) where the level of that Anomaly Detection Threshold is no longer appropriate, set a new Anomaly Detection Threshold in accordance with the relevant provisions of this Section G6.

G7. SECURITY SUB-COMMITTEE

Establishment of the Security Sub-Committee

G7.1 The Panel shall establish a Sub-Committee in accordance with the requirements of this Section G7, to be known as the "**Security Sub-Committee**".

G7.2 Save as expressly set out in this Section G7, the Security Sub-Committee shall be subject to the provisions concerning Sub-Committees set out in Section C6 (Sub- Committees).

Membership of the Security Sub-Committee

G7.3 The Security Sub-Committee shall be composed of the following persons (each a "**Security Sub-Committee Member**"):

(a) the Security Sub-Committee Chair (as further described in Section G7.5);

(b) eight Security Sub-Committee (Supplier) Members (as further described in Section G7.6);

(c) two Security Sub-Committee (Network) Members (as further described in Section G7.8);

(d) one Security Sub-Committee (Other User) Member (as further described in Section G7.10);

(e) one Security Sub-Committee (Shared Resource Provider) Member (as further described in Section G7.12);

(f) one representative of the DCC (as further described in Section G7.15).

G7.4 Each Security Sub-Committee Member must be an individual (and cannot be a body corporate, association or partnership). No one person can hold more than one office as a Security Sub-Committee Member at the same time.

G7.5 The "**Security Sub-Committee Chair**" shall be such person as is (from time to time) appointed to that role by the Panel in accordance with a process designed to ensure that:

(a) the candidate selected is sufficiently independent of any particular Party or class of Parties;

(b) the Security Sub-Committee Chair is appointed for a three-year term (following which he or she can apply to be re-appointed);

(c) the Security Sub-Committee Chair is remunerated at a reasonable rate;

(d) the Security Sub-Committee Chair's appointment is subject to Section C6.9 (Member Confirmation), and to terms equivalent to Section C4.6 (Removal of Elected Members);

(e) provision is made for the Security Sub-Committee Chair to continue in office for a reasonable period following the end of his or her term of office in the event of any delay in appointing his or her successor; and

(f) where the Security Sub-Committee Chair's appointment (and for the purposes of this Section and Section G7.5A all references to appointment shall encompass re-appointment) is to take effect on or after the date this Section G7.5(f) comes into force, the Panel shall:

(i) notify the Secretary of State of the appointment it proposes to make;

(ii) not make the appointment unless and until the Secretary of State has confirmed in writing that they do not object to the appointment being made;

(iii) ensure that the terms of the appointment include terms which provide for the Panel to terminate the appointment where directed to do so by the Secretary of State pursuant to Section G7.5A and from such date or within such period as may be specified in the Secretary of State's direction; and

(iv) where the appointed person has not, at the date of the appointment, passed (as a minimum) a Security Check (or equivalent), ensure that the terms of the appointment include terms which:

(A) require the appointed person to apply for a Security Check (or equivalent) within one month of the date of the appointment;

(B) provide for the Panel to terminate the appointment if a Security Check (or equivalent) is not passed by the appointed person within 12 months of the date of the appointment (or such longer period as the Secretary of State may approve following a request from the Panel).

G7.5A The Secretary of State may, in respect of any Security Sub-Committee Chair appointment which takes effect on or after the date Section G7.5(f) comes into force, direct the Panel to terminate the appointment of the Security Sub-Committee Chair where the Secretary of State considers it necessary to do for the purposes of preserving the integrity of, and in the interests of maintaining, the security of the End-to-End Smart Metering System (or any part of that system).

G7.5B The Panel shall comply with any direction given to it by the Secretary of State pursuant to Section G7.5A.

G7.6 Each of the eight "**Security Sub-Committee (Supplier) Members**" shall (subject to any directions to the contrary made by the Secretary of State for the purpose of transition on the incorporation of this Section G7 into this Code):

(a) be appointed in accordance with Section G7.7, subject to compliance by the appointed person with Section C6.9 (Member Confirmation);

(b) retire two years after his or her appointment (without prejudice to his or her ability to be nominated for a further term of office); and

(c) be capable of being removed from office in accordance with Sections C4.5 and C4.6 (Removal of Elected Members), for which purpose those Sections shall be read as if references to "Elected Member" were to "Security Sub-Committee (Supplier) Member", references to "Panel" were to "Security Sub-Committee", references to "Panel Chair" were to "Security Sub-Committee Chair", and references to "Panel Members" were to "Security Sub-Committee Members".

G7.7 Each of the eight Security Sub-Committee (Supplier) Members shall (subject to Section G7.14) be appointed in accordance with a process:

(a) by which six Security Sub-Committee (Supplier) Members will be elected by Large Supplier Parties, and two Security Sub-Committee (Supplier) Members will be elected by Small Supplier Parties; and

(b) that is otherwise the same as that by which Elected Members are elected under Sections C4.2 and C4.3 (as if references therein to "Panel" were to "Security Sub-Committee", references to "Panel Chair" were to "Security Sub-Committee Chair", references to "Panel Members" were to "Security Sub-Committee Members", and references to provisions of Section C or D were to the corresponding provisions set out in or applied pursuant to this Section G7).

G7.8 Each of the two "**Security Sub-Committee (Network) Members**" shall (subject to any directions to the contrary made by the Secretary of State for the purpose of transition on the incorporation of this Section G7 into this Code):

(a) be appointed in accordance with Section G7.9, subject to compliance by the appointed person with Section C6.9 (Member Confirmation);

(b) retire two years after his or her appointment (without prejudice to his or her ability to be nominated for a further term of office); and

(c) be capable of being removed from office in accordance with Sections C4.5 and C4.6 (Removal of Elected Members), for which purpose those Sections shall be read as if references to "Elected Member" were to "Security Sub-Committee (Network) Member", references to "Panel" were to "Security Sub-Committee", references to "Panel Chair" were to "Security Sub-Committee Chair", and references to "Panel Members" were to "Security Sub-Committee Members".

G7.9 Each of the two Security Sub-Committee (Network) Members shall (subject to Section G7.14) be appointed in accordance with a process:

(a) by which one Security Sub-Committee (Network) Member will be elected by the Electricity Network Parties and one Security Sub-Committee (Network) Member will be elected by the Gas Network Parties; and

(b) that is otherwise the same as that by which Elected Members are elected under Sections C4.2 and C4.3 (as if references therein to “Panel” were to “Security Sub-Committee”, references to “Panel Chair” were to “Security Sub-Committee Chair”, references to “Panel Members” were to “Security Sub-Committee Members”, and references to provisions of Section C or D were to the corresponding provisions set out in or applied pursuant to this Section G7).

G7.10 The “**Security Sub-Committee (Other User) Member**” shall (subject to any directions to the contrary made by the Secretary of State for the purpose of transition on the incorporation of this Section G7 into this Code):

(a) be appointed in accordance with Section G7.11, subject to compliance by the appointed person with Section C6.9 (Member Confirmation);

(b) retire two years after his or her appointment (without prejudice to his or her ability to be nominated for a further term of office); and

(c) be capable of being removed from office in accordance with Sections C4.5 and C4.6 (Removal of Elected Members), for which purpose those Sections shall be read as if references to “Elected Member” were to “Security Sub-Committee (Other User) Member”, references to “Panel” were to “Security Sub- Committee”, references to “Panel Chair” were to “Security Sub-Committee Chair”, and references to “Panel Members” were to “Security Sub-Committee Members”.

G7.11 The Security Sub-Committee (Other User) Member shall (subject to Section G7.14) be appointed in accordance with a process:

(a) by which he or she is elected by those Other SEC Parties which are Other Users; and

(b) that is otherwise the same as that by which Elected Members are elected under Sections C4.2 and C4.3 (as if references therein to “Panel” were to “Security Sub-Committee”, references to “Panel Chair” were to “Security Sub-Committee Chair”, references to “Panel Members” were to “Security Sub-Committee Members”, and references to provisions of Section C or D were to the corresponding provisions set out in or applied pursuant to this Section G7).

G7.12 The “**Security Sub-Committee (Shared Resource Provider) Member**” shall:

(a) be appointed in accordance with Section G7.13, subject to compliance by the appointed person with Section C6.9 (Member Confirmation);

(b) retire two years after his or her appointment (without prejudice to his or her ability to be nominated for a further term of office); and

(c) be capable of being removed from office in accordance with Sections C4.5 and C4.6 (Removal of Elected Members), for which purpose those Sections shall be read as if references to “Elected Member” were to “Security Sub-Committee (Shared Resource Provider) Member”, references to “Panel” were to “Security Sub-Committee”, references to “Panel Chair” were to “Security Sub-Committee Chair”, and references to “Panel Members” were to “Security Sub-Committee Members”.

G7.13 The Security Sub-Committee (Shared Resource Provider) Member shall (subject to Section G7.14) be appointed in accordance with a process:

(a) by which he or she is elected by those Other SEC Parties which are Shared Resource Providers; and

(b) that is otherwise the same as that by which Elected Members are elected under Sections C4.2 and C4.3 (as if references therein to “Panel” were to “Security Sub-Committee”, references to “Panel Chair” were to “Security Sub-Committee Chair”, references to “Panel Members” were to “Security Sub-Committee Members”, and references to provisions of Section C or D were to the corresponding provisions set out in or applied pursuant to this Section G7).

G7.14 The following shall apply in respect of all candidates nominated or re-nominated for election as a Security Sub-Committee (Supplier) Member, Security Sub-Committee (Network) Member, Security Sub-Committee (Other User) Member or Security Sub- Committee (Shared Resource Provider) Member:

(a) the Security Sub-Committee may, by no later than 5 Working Days following the expiry of the period of time set out in the request for nominations, reject a candidate (by notifying the candidate of such rejection) where the Security Sub-Committee determines that the candidate does not satisfy one or more of the following requirements:

(i) the candidate must have been nominated by a company or other organisation, and the individual who submitted the nomination on behalf of the organisation must hold a senior position within the organisation;

(ii) the organisation which nominated the candidate must have confirmed that it is satisfied that the candidate has the relevant security expertise in relation to the category of membership of the Security Sub- Committee for which the candidate has been nominated;

(iii) the organisation which nominated the candidate must have confirmed that the candidate has successfully completed a BS7858 security assessment (or a security assessment named by such organisation which the organisation confirms to be equivalent); and

(iv) the candidate must have sufficient security expertise in relation to the category of membership of the Security Sub-Committee for which the candidate has been nominated;

(b) a candidate who is rejected under paragraph (a) above shall not (subject to paragraph (c) below) be an eligible candidate for the relevant election;

(c) where a candidate disputes a rejection notification under paragraph (a) above, the candidate shall have 3 Working Days following receipt of such notification to refer the matter to the Panel for its final determination of whether the candidate satisfies the requirements set out in paragraph (a) above; and

(d) where necessary, the Secretariat shall delay giving notice of the names of eligible candidates pending expiry of the time periods set out in paragraph (a) and/or (c) or determination by the Panel under paragraph (c) (as applicable).

G7.15 The DCC may nominate one person to be a Security Sub-Committee Member by notice to the Secretariat from time to time. The DCC may replace its nominee from time to time by prior notice to the Secretariat. Such nomination or replacement shall be subject to compliance by the relevant person with Section C6.9 (Member Confirmation).

Proceedings of the Security-Sub Committee

G7.16 Without prejudice to the generality of Section C5.13(c) (Attendance by Other Persons) as it applies pursuant to Section G7.17:

(a) a representative of the Secretary of State and a representative of the Authority shall be:

(i) invited to attend each and every Security Sub-Committee meeting;

(ii) entitled to speak at such Security Sub-Committee meetings without the permission of the Security Sub-Committee Chair; and

(iii) provided with copies of all the agenda and supporting papers available to Security Sub-Committee Members in respect of such meetings;

(b) the Security Sub-Committee Chair shall invite to attend Security Sub- Committee meetings any persons that the Security Sub-Committee determines it appropriate to invite in order to be provided with expert advice on security matters.

G7.17 Subject to Section G7.16, the provisions of Section C5 (Proceedings of the Panel) shall apply to the proceedings of the Security Sub-Committee, for which purpose that Section shall be read as if references to “Panel” were to “Security Sub-Committee”, references to “Panel Chair” were to “Security Sub-Committee Chair”, and references to “Panel Members” were to “Security Sub-Committee Members”.

Duties and Powers of the Security Sub-Committee

G7.18 The Security Sub-Committee:

(a) shall perform the duties and may exercise the powers set out in Sections G7.19 to G7.23; and

(b) shall perform such other duties and may exercise such other powers as may be expressly ascribed to the Security Sub-Committee elsewhere in this Code.

Document Development and Maintenance

G7.19 The Security Sub-Committee shall:

(a) develop and maintain documents, to be known as the "**Security Controls Framework**", which shall set out the appropriate User and DCC Security Assessment Methodology to be applied to different categories of security assurance assessment carried out in accordance with Section G8 (User Security Assurance) and Section G9 (DCC Security Assurance) and be designed to ensure that such security assurance assessments are proportionate; and

(i) achieve appropriate levels of security assurance in respect of different Users and different User Roles, and the DCC; and

(ii) in the case of User related assessments are consistent in their treatment of equivalent Users and equivalent User Roles, and;

(b) carry out reviews of the Security Risk Assessment:

(i) at least once each year in order to identify any new or changed security risks to the End-to-End Smart Metering System; and

(ii) in any event promptly if the Security Sub-Committee considers there to be any material change in the level of security risk;

(c) maintain the Security Requirements to ensure that it is up to date and at all times identifies the security controls which the Security Sub-Committee considers appropriate to mitigate the security risks identified in the Security Risk Assessment;

(d) maintain the End-to-End Security Architecture to ensure that it is up to date;

(e) develop and maintain a document to be known as the "**Risk Treatment Plan**", which shall identify the residual security risks which in the opinion of the Security Sub-Committee remain unmitigated taking into account the security controls that are in place;

(f) liaise and work with the NCSC to develop and maintain CPA Security Characteristics that set out the levels of security required for Smart Meters, Communications Hubs, SAPCs and HCALCs that are proportionate and appropriate taking into consideration the security risks identified in the Security Risk Assessment; and

(g) develop and maintain documents to be known as "**SSC Guidance for Device Security Assurance and Triage**" which shall set out the SSC's guidance on the requirements and processes to be followed in respect of Devices (including their triage and refurbishment) in order to:

(i) achieve appropriate levels of security assurance in accordance with the requirement of this Code; and

(ii) obtain and maintain CPA Certification.

Security Assurance

G7.20 The Security Sub-Committee shall:

(a) periodically, and in any event at least once each year, review the Security Obligations and Assurance Arrangements in order to identify whether in the opinion of the Security Sub-Committee they continue to be fit for purpose;

(b) exercise such functions as are allocated to it under, and comply with the applicable requirements of Section G8 (User Security Assurance) and Section G9 (DCC Security Assurance);

(c) provide the Panel with support and advice in respect of issues relating to the actual or potential non-compliance of any Party with the requirements of the Security Obligations and Assurance Arrangements;

(d) keep under review the NCSC CPA Certificate scheme in order to assess whether it continues to be fit for purpose in so far as it is relevant to the Code, and suggest modifications to the scheme provider to the extent to which it considers them appropriate;

(e) to the extent to which it considers it appropriate, in relation to any User (or, during the first User Entry Process, Party) which has produced a User Security Assessment Response that sets out any steps that the User proposes to take in accordance with Section G8.24(b):

(i) liaise with that User (or Party) as to the nature and timetable of such steps;

(ii) either accept the proposal to take those steps within that timetable or seek to agree with that User (or Party) such alternative steps or timetable as the Security Sub-Committee may consider appropriate; and

(iii) take advice from the User Independent Security Assurance Service Provider; and

(iv) where the Security Sub-Committee considers it appropriate, request the User Independent Security Assurance Service Provider to carry out a Follow-up Security Assessment;

(f) provide advice to the Panel on the scope and output of the independent security assurance arrangements of the DCC in relation to the design, building and testing of the DCC Total System;

(g) to the extent to which it considers appropriate, in relation to the DCC which has produced a DCC Security Assessment Response that sets out any steps that the DCC proposes to take in accordance with Section G9.24(b):

(i) liaise with the DCC as to the nature and timetable of such steps;

(ii) either accept the proposal to take those steps within that timetable or seek to agree with the DCC such alternative steps or timetable as the Security Sub-Committee may consider appropriate;

(iii) take advice from the DCC Independent Security Assessment Service Provider; and

(iv) where the Security Sub-Committee considers it appropriate, request the DCC Independent Security Assessment Service Provider to carry out a Follow-up Security Assessment;

(h) provide advice to the:

(i) Panel in relation to the appointment of the User Independent Security Assurance Service Provider, monitor the performance of the person appointed to that role and provide advice to the Panel in respect of its views as to that performance; and

(ii) DCC in relation to the appointment of the DCC Independent Security Assessment Service Provider, monitor the performance of the person appointed to that role and provide advice to the DCC in respect of its views as to that performance;

(i) provide advice and information to the Authority in relation to any actual or potential non-compliance with the CPA Security Characteristics of any Device or apparatus in respect of which a CPA Certificate is issued or required.

Monitoring and Advice

G7.21 The Security Sub-Committee shall:

(a) provide such reasonable assistance to the DCC and Users as may be requested by them in relation to the causes of security incidents and the management of vulnerabilities on their Systems;

(b) monitor the (actual and proposed) Anomaly Detection Thresholds of which it is notified by the DCC, consider the extent to which they act as an effective means of detecting any Compromise to any relevant part of the DCC Total System or of any User Systems, and provide its opinion on such matters to the DCC;

(c) provide the Panel with support and advice in respect of Disputes for which the Panel is required to make a determination, insofar as such Disputes relate to the Security Obligations and Assurance Arrangements;

(d) provide the Panel, the Change Sub-Committee, the Change Board and any relevant Working Group with support and advice in relation to any Draft Proposal or Modification Proposal which may affect the security of the End-to- End Smart Metering System or the effective implementation of the security controls that are identified in the Security Requirements;

(e) advise the Authority of any modifications to the conditions of Energy Licences which it considers may be appropriate having regard to the residual security risks identified from time to time in the Risk Treatment Plan;

(f) respond to any consultations on matters which may affect the security of the End-to-End Smart Metering System or the effective implementation of the security controls that are identified in the Security Requirements;

(g) act in cooperation with, and send a representative to, the SMKI PMA, the Technical Architecture and Business Architecture Sub-Committee and any other Sub-Committee or Working Group which requests the support or attendance of the Security Sub-Committee;

(h) (to the extent to which it reasonably considers that it is necessary to do so) liaise and exchange information with, provide advice to, and seek the advice of the At HAN Forum on matters relating to the Alt HAN Arrangements which may affect the security of the End-to-End Smart Metering System or the effective implementation of the security controls that are identified in the Security Requirements;

(i) provide such further support and advice to the Panel as it may request; and

(j) provide the Authority with such information and documents as it may reasonably request in relation to any matter referred by a Party to the Authority for determination pursuant to Section F2.7B.

Modifications

G7.22 The Security Sub-Committee shall establish a process under which the Code Administrator monitors Draft Proposals and Modification Proposals with a view to identifying (and bringing to the attention of the Security Sub-Committee) those proposals that:

(a) are likely to affect the Security Obligations and Assurance Arrangements; or

(b) are likely to relate to other parts of the Code but may have a material effect on the security of the End-to-End Smart Metering System,

and the Code Administrator shall comply with such process.

G7.23 Notwithstanding Section D1.3 (Persons Entitled to Submit Draft Proposals):

(a) the Security Sub-Committee shall be entitled to submit Draft Proposals in respect of the Security Obligations and Assurance Arrangements where the Security Sub-Committee considers it appropriate to do so; and

(b) any Security Sub-Committee Member shall be entitled to submit Draft Proposals in respect of the Security Obligations and Assurance Arrangements where he or she considers it appropriate to do so (where the Security Sub-Committee has voted not to do so).

G7.24 Notwithstanding and subject to the provisions of the Working Group Terms of Reference, the Security Sub-Committee shall be entitled to nominate a representative to be a member of any Working Group.

G7.25 For the purposes of Section D7.1 (Modification Report):

(a) written representations in relation to the purpose and effect of a Modification Proposal may be made by:

(i) the Security Sub-Committee; and/or

(ii) any Security Sub-Committee Member (either alone or in addition to any representations made by other Security Sub-Committee Members and/or the Security Sub-Committee collectively); and

(b) notwithstanding Section D7.3 (Content of the Modification Report), the Code Administrator shall ensure that all such representations, and a summary of any evidence provided in support of them, are set out in the Modification Report prepared in respect of the relevant Modification Proposal.

G8. USER SECURITY ASSURANCE

Procurement of the User Independent Security Assurance Service Provider

G8.1 The Panel shall procure the provision of security assurance services:

(a) of the scope specified in Section G8.3;

(b) from a person who:

(i) is suitably qualified in accordance with Section G8.4;

(ii) is suitably independent in accordance with Section G8.7; and

(iii) satisfies the capacity requirement specified in Section G8.11,

(c) and that person is referred to in this Section G8 as the "**User Independent Security Assurance Service Provider**".

G8.2 The Panel may appoint more than one person to carry out the functions of the User Independent Security Assurance Service Provider.

Scope of Security Assurance Services

G8.3 The security assurance services specified in this Section G8.3 are services in accordance with which the User Independent Security Assurance Service Provider shall:

(a) carry out User Security Assessments at such times and in such manner as is provided for in this Section G8;

(b) produce User Security Assessment Reports in relation to Users that have been the subject of a User Security Assessment;

(c) receive and consider User Security Assessment Responses and carry out any Follow-up Security Assessments at the request of the Security Sub-Committee;

(d) otherwise, at the request of, and to an extent determined by, the Security Sub- Committee, carry out an assessment of the compliance of any User with its obligations under Sections G3 to G6 where:

(i) following either a User Security Self-Assessment or Verification User Security Assessment, any material increase in the security risk relating to that User has been identified; or

(ii) the Security Sub-Committee otherwise considers it appropriate for that assessment to be carried out;

(e) review the outcome of User Security Self-Assessments;

(f) at the request of the Security Sub-Committee, provide to it advice in relation to:

(i) the compliance of any User with its obligations under Sections G3 to G6 or any CPA Certificate Remedial Plan; and

(ii) changes in security risks relating to the Systems, Data, functionality and processes of any User which fall within Section G5.14 (Information Security: Obligations on Users);

(g) at the request of the Panel, provide to it advice in relation to the suitability of any remedial action plan for the purposes of Section M8.4 of the Code (Consequences of an Event of Default);

(h) at the request of the Security Sub-Committee Chair, provide a representative to attend and contribute to the discussion at any meeting of the Security Sub-Committee; and

(i) undertake such other activities, and do so at such times and in such manner, as may be further provided for in this Section G8.

Suitably Qualified Service Provider

G8.4 The User Independent Security Assurance Service Provider shall be treated as suitably qualified in accordance with this Section G8.4 only if it satisfies:

(a) the requirements specified in Section G8.5; and

(b) the requirements specified in Section G8.6.

G8.5 The requirements specified in this Section G8.5 are that the User Independent Security Assurance Service Provider:

(a) is accredited by UKAS as meeting the requirements for providing audit and certification of information security management systems in accordance with ISO/IEC 27001:2013 (Information

Technology – Security Techniques – Information Security Management Systems) or any equivalent to that standard which updates or replaces it from time to time; and/or

(b) holds another membership, accreditation, approval or form of professional validation that is in the opinion of the Security Sub-Committee substantially equivalent in status and effect to the arrangements described in paragraph (a).

G8.6 The requirement specified in this Section G8.6 is that the User Independent Security Assurance Service Provider:

(a) employs consultants who are assured under an official cyber security qualification scheme recognised by NCSC or the UK Cyber Security Council or UKAS and which is approved by the Security Sub-Committee at levels equivalent to 'Chartered', 'Principal', 'Lead' or 'Senior Practitioner' in either the 'Security and Information Risk Advisor' or 'Information Assurance Auditor' roles; and

(b) engages those individuals as its lead auditors for the purposes of carrying out all security assurance assessments in accordance with this Section G8.

Independence Requirement

G8.7 The User Independent Security Assurance Service Provider shall be treated as suitably independent in accordance with this Section G8.7 only if it satisfies:

(a) the requirements specified in Section G8.9; and

(b) the requirement specified in Section G8.10.

G8.8 For the purposes of Sections G8.9 and G8.10:

(a) a "**Relevant Party**" means any Party in respect of which the User Independent Security Assurance Service Provider carries out functions under this Section G8; and

(b) a "**Relevant Service Provider**" means any service provider to a Relevant Party from which that Party acquires capability for a purpose related to its compliance with its obligations as a User under Sections G3 to G6.

G8.9 The requirements specified in this Section G8.9 are that:

(a) no Relevant Party or any of its subsidiaries, and no Relevant Service Provider or any of its subsidiaries, holds or acquires any investment by way of shares, securities or other financial rights or interests in the User Independent Security Assurance Service Provider;

(b) no director of any Relevant Party, and no director of any Relevant Service Provider, is or becomes a director or employee of, or holds or acquires any investment by way of shares, securities or other financial rights or interests in, the User Independent Security Assurance Service Provider; and

(c) the User Independent Security Assurance Service Provider does not hold or acquire a participating interest (as defined in section 421A of the Financial Services and Markets Act 2000) in any Relevant Party or any Relevant Service Provider,

(but for these purposes references to a Relevant Service Provider shall not include the User Independent Security Assurance Service Provider where it acts in that capacity).

G8.10 The requirement specified in this Section G8.10 is that the User Independent Security Assurance Service Provider is able to demonstrate to the satisfaction of the Panel that it has in place arrangements to ensure that it will at all times act independently of any commercial relationship that it has, has had, or may in future have with a Relevant Party or Relevant Service Provider (and for these purposes a 'commercial relationship' shall include a relationship established by virtue of the User Independent Security Assurance Service Provider itself being a Relevant Service Provider to any Relevant Party).

Capacity Requirement

G8.11 The capacity requirement specified in this Section G8.11 is that the User Independent Security Assurance Service Provider must be capable of meeting the Panel's estimate of the demand for its security assurance services throughout the period in relation to which those services are being procured.

Compliance of the User Independent Security Assurance Service Provider

G8.12 The Panel shall be responsible for ensuring that the User Independent Security Assurance Service Provider carries out its functions in accordance with the provisions of this Section G8.

Users: Duty to Cooperate in Assessment

G8.13 Each User shall do all such things as may be reasonably requested by the Security Sub- Committee, or by any person acting on behalf of or at the request of the Security Sub- Committee (including in particular the User Independent Security Assurance Service Provider), for the purposes of facilitating an assessment of that User's compliance with its obligations under Sections G3 to G6 or any CPA Certificate Remedial Plan.

G8.14 For the purposes of Section G8.13, a User shall provide the Security Sub-Committee (or the relevant person acting on its behalf or at its request) with:

(a) all such Data as may reasonably be requested, within such times and in such format as may reasonably be specified;

(b) all such other forms of cooperation as may reasonably be requested, including in particular:

(i) access at all reasonable times to such parts of the premises of that User as are used for, and such persons engaged by that User as carry out or are authorised to carry out, any activities related to its compliance with its obligations under Sections G3 to G6; and

(ii) such cooperation as may reasonably be requested by the Independent Security Assessment Services Provider for the purposes of carrying out any security assurance assessment in accordance with this Section G8.

Categories of Security Assurance Assessment

G8.15 For the purposes of this Section G8, there shall be the following four categories of security assurance assessment:

(a) a Full User Security Assessment (as further described in Section G8.16);

(b) a Verification User Security Assessment (as further described in Section G8.17);

(c) a User Security Self-Assessment (as further described in Section G8.18); and

(d) a Follow-up Security Assessment (as further described in Section G8.19).

G8.16 A "**Full User Security Assessment**" shall be an assessment carried out by the User Independent Security Assurance Service Provider in respect of a User to identify the extent to which that User is compliant with each of its obligations under Sections G3 to G6 in each of its User Roles.

G8.17 A "**Verification User Security Assessment**" shall be an assessment carried out by the User Independent Security Assurance Service Provider in respect of a User to identify any material increase in the security risk relating to the Systems, Data, functionality and processes of that User falling within Section G5.14 (Information Security: Obligations on Users) since the last occasion on which a Full User Security Assessment was carried out in respect of that User.

G8.18 A "**User Security Self-Assessment**" shall be an assessment carried out by a User, the outcome of which is reviewed by the User Independent Security Assurance Service Provider, to identify any material increase in the security risk relating to the Systems, Data, functionality and processes of that User falling within Section G5.14 (Information Security: Obligations on Users) since the last occasion on which a User Security Assessment was carried out in respect of that User.

G8.19 A "**Follow-up Security Assessment**" shall be an assessment carried out by the User Independent Security Assurance Service Provider, following a User Security Assessment, in accordance with the provisions of Section G8.29.

G8.20 For the purposes of Sections G8.17 and G8.18, a Verification Security Assessment and User Security Self-Assessment shall each be assessments carried out in respect of a User having regard in particular to:

(a) any changes made to any System, Data, functionality or process falling within the scope of Section G5.14 (Information Security: Obligations on Users);

(b) where the User is a Supplier Party, any increase in the number of Enrolled Smart Metering Systems for which it is the Responsible Supplier; and

(c) where the User is a Network Party, any increase in the number of Enrolled Smart Metering Systems for which it is the Electricity Distributor or the Gas Transporter.

User Security Assessments: General Procedure

User Security Assessment Methodology

G8.21 Each User Security Assessment carried out by the User Independent Security Assurance Service Provider shall be carried out in accordance with the User Security Assessment Methodology applicable to the relevant category of assessment.

The User Security Assessment Report

G8.22 Following the completion of a User Security Assessment, the User Independent Security Assurance Service Provider shall, in discussion with the User to which the assessment relates, produce a written report (a "**User Security Assessment Report**") which shall:

(a) set out the findings of the User Independent Security Assurance Service Provider on all the matters within the scope of the User Security Assessment;

(b) in the case of a Full User Security Assessment:

(i) specify any instances of actual or potential non-compliance of the User with its obligations under Sections G3 to G6 which have been identified by the User Independent Security Assurance Service Provider; and

(ii) set out the evidence which, in the opinion of the User Independent Security Assurance Service Provider, establishes each of the instances of actual or potential non-compliance which it has identified; and

(c) in the case of a Verification User Security Assessment:

(i) specify any material increase in the security risk relating to that User which the User Independent Security Assurance Service Provider has identified since the last occasion on which a Full User Security Assessment was carried out in respect of that User; and

(ii) set out the evidence which, in the opinion of the User Independent Security Assurance Service Provider, establishes the increase in security risk which it has identified.

G8.23 The User Independent Security Assurance Service Provider shall submit a copy of each User Security Assessment Report to the Security Sub-Committee and to the User to which that report relates.

The User Security Assessment Response

G8.24 Following the receipt by any User of a User Security Assessment Report which relates to it, the User shall as soon as reasonably practicable, and in any event by no later than such date as the Security Sub-Committee may specify:

(a) produce a written response to that report (a "**User Security Assessment Response**") which addresses the findings set out in the report; and

(b) submit a copy of that response to the Security Sub-Committee and the User Independent Security Assurance Service Provider.

G8.25 Where a User Security Assessment Report:

(a) following a Full User Security Assessment, specifies any instance of actual or potential non-compliance of a User with its obligations under Sections G3 to G6; or

(b) following a Verification User Security Assessment, specifies any material increase in the security risk relating to a User since the last occasion on which a Full User Security Assessment was carried out in respect of that User,

the User shall ensure that its User Security Assessment Response includes the matters referred to in Section G8.26.

G8.26 The matters referred to in this Section are that the User Security Assessment Response:

(a) indicates whether the User accepts the relevant findings of the User Independent Security Assurance Service Provider and, where it does not, explains why this is the case;

(b) sets out any steps that the User has taken or proposes to take in order to remedy and/or mitigate the actual or potential non-compliance or the increase in security risk (as the case may be) specified in the User Security Assessment Report; and

(c) identifies a timetable within which the User proposes to take any such steps that have not already been taken.

G8.27 Where a User Security Assessment Response sets out any steps that the User proposes to take in accordance with Section G8.26(b), the Security Sub-Committee (having considered the advice of the User Independent Security Assurance Service Provider) shall review that response and either:

(a) notify the User that it accepts that the steps that the User proposes to take, and the timetable within which it proposes to take them, are appropriate to remedy and/or mitigate the actual or potential non-compliance or increase in security risk (as the case may be) specified in the User Security Assessment Report; or

(b) seek to agree with the User such alternative steps and/or timetable as would, in the opinion of the Security Sub-Committee, be more appropriate for that purpose.

G8.28 Where a User Security Assessment Response sets out any steps that the User proposes to take in accordance with Section G8.26(b), and where those steps and the timetable within which it proposes to take them are accepted by the Security Sub-Committee, or alternative steps and/or an alternative timetable are agreed between it and the User in accordance with Section G8.27, the User shall:

(a) take the steps that have been accepted or agreed (as the case may be) within the timetable that has been accepted or agreed (as the case may be); and

(b) report to the Security Sub-Committee on:

(i) its progress in taking those steps, at any such intervals or by any such dates as the Security Sub-Committee may specify;

(ii) the completion of those steps in accordance with the timetable; and

(iii) any failure to complete any of those steps in accordance with the timetable, specifying the reasons for that failure.

Follow-up Security Assessment

G8.29 Where a User Security Assessment Response sets out any steps that the User proposes to take in accordance with Section G8.26(b), and where those steps and the timetable within which it proposes to take them are accepted by the Security Sub-Committee, or alternative steps and/or an alternative timetable are agreed between it and the User in accordance with Section G8.27, the User Independent Security Assurance Service Provider shall, at the request of the Security Sub-Committee (and by such date as it may specify), carry out a Follow-up Security Assessment of the relevant User to:

(a) identify the extent to which the User has taken the steps that have been accepted or agreed (as the case may be) within the timetable that has been accepted or agreed (as the case may be); and

(b) assess any other matters related to the User Security Assessment Response that are specified by the Security Sub-Committee.

User Security Assessments: Further Provisions

G8.30 The User Independent Security Assurance Service Provider:

(a) may in its discretion, and shall where directed to do so by the Security Sub- Committee:

(i) in relation to a User which acts in more than one User Role, determine that a single User Security Assessment may be carried out in relation to that User in respect of any two or more such User Roles; and

(ii) in carrying out any User Security Assessment, take into account any relevant security accreditation or certification held by the relevant User; and

(b) shall, where any Shared Resources which have not been provided by a Shared Resource Provider form part of the User Systems of more than one User, have regard to information obtained in relation to such Shared Resources in the User Security Assessment of one such User when carrying out a User Security Assessment of any other such User.

Initial Full User Security Assessment: User Entry Process

G8.31 Sections G8.33 to G8.39 set out the applicable security requirements referred to in Section H1.10(c) (User Entry Process Requirements).

G8.32 For the purposes of Sections G8.33 to G8.39, any reference in Sections G3 to G6 or the preceding provisions of this Section G8 to a 'User' (or to any related expression which applies to Users), shall be read as including a reference (or otherwise applying) to any Party seeking to become a User by completing the User Entry Process for any User Role.

Initial Full User Security Assessment

G8.33 For the purpose of completing the User Entry Process for a User Role, a Party wishing to act as a User in that User Role shall be subject to a Full User Security Assessment in respect of the User Role.

Panel: Setting the Assurance Status

G8.34 Following the completion of that initial Full User Security Assessment, the Security Sub-Committee shall ensure that copies of both the User Security Assessment Report and User Security Assessment Response are provided to the Panel.

G8.35 Following the receipt by it of the User Security Assessment Report and User Security Assessment Response, the Panel shall promptly consider both documents and (having regard to any advice of the Security Sub-Committee) set the assurance status of the Party, in relation to its compliance with each of its obligations under Sections G3 to G6 in the relevant User Role, in accordance with Section G8.36.

G8.36 The Panel shall set the assurance status of the Party as one of the following:

(a) approved;

(b) approved, subject to the Party:

(i) taking such steps as it proposes to take in its User Security Assessment Response in accordance with Section G8.26(b); or

(ii) both taking such steps and being subject to a Follow-up Security Assessment by such date as the Panel may specify,

(c) deferred and:

(i) the Party having first taken such steps as it proposes to take in its User Security Assessment Response in accordance with Section G8.26(b) and been subject to a Follow-up Security Assessment; and

(ii) the Panel having determined that it is satisfied, on the evidence of the Follow-up Security Assessment, that such steps have been taken; or

(d) rejected and:

(i) the Party shall have a second Full User Security Assessment to address any issues identified by the Panel as being, in the opinion of the Panel, not adequately addressed in that response as submitted to the Security Sub-Committee; and

(ii) upon completion of the second Full User Security Assessment the Panel will reconsider the assurance status in accordance with Section G8.35.

Approval

G8.37 For the purposes of Sections H1.10(c) and H1.11 (User Entry Process Requirements):

(a) a Party shall be considered to have successfully demonstrated that it meets the applicable security requirements of this Section G8 when:

(i) the Panel has set its assurance status to 'approved' in accordance with either Section G8.36(a) or (b); or

(ii) the Panel has set its assurance status to 'deferred' in accordance with Section G8.36(c) and the requirements specified in that Section have been met; and

(b) the Panel shall notify the Code Administrator as soon as reasonably practicable after the completion of either event described in paragraph (a)(i) or (ii).

Obligations on an Approved Party

G8.38 Where the Panel has set the assurance status of a Party to 'approved subject to' specified in Section G8.36(b), the Party shall take the steps to which that approval is subject in accordance with that section.

Disagreement with Panel Decisions

G8.39 Where a Party disagrees with any decision made by the Panel in relation to it under Section G8.36, it may appeal that decision to the Authority and the determination of the Authority shall be final and binding for the purposes of the Code.

Security Assurance Assessments: Post-User Entry Process

G8.40 Within 12 months after completion of the User's initial Full User Security Assessment (or after the Follow-up Security Assessment where there was one), for the purposes of the User Entry Process, a User shall schedule a User Security Assessment with the User Independent Security Assurance Provider in accordance with the provisions of Sections G8.41 to G8.47. The initial Full User Security Assessment will be deemed complete when the Panel set an assurance status of:

(a) approved; or

(b) approved, subject to the User:

(i) taking such steps as the User proposes to take in its User Security Assessment Response in accordance with Section G8.26(b); or

(ii) both taking the steps referred to in (i) above and being subject to a Follow-up Security Assessment by such date as the Panel may specify.

Supplier Parties

G8.41 Where a User is a Supplier Party and either:

(a) the number of Domestic Premises supplied with electricity and/or gas through one or more Smart Metering Systems for which it is the Responsible Supplier exceeds 250,000; or

(b) the number of Non-Domestic Premises supplied with electricity and/or gas through one or more Smart Metering Systems for which it is the Responsible Supplier exceeds 50,000; or

(c) $(5N) + D > 250,000$

Where N is the number of Non-Domestic Premises and D is the number of Domestic Premises supplied with electricity and/or gas through one or more Smart Metering Systems for which it is the Responsible Supplier,

the User Security Assessment required by Section G8.40 shall be a Full User Security Assessment and the User shall schedule a further Full User Security Assessment within 12 months after each Full User Security Assessment.

G8.42 Where a User is a Supplier Party of electricity and/or gas to Domestic Premises and/or Non-Domestic Premises through one or more Smart Metering Systems for which it is the Responsible Supplier but does not meet any of the criteria specified under Section G8.41, the User Security Assessment required by Section G8.40 shall be a Verification User Security Assessment and the User shall:

(a) within 12 months after each Verification User Security Assessment schedule a User Security Self-Assessment; and

(b) within 12 months after each User Security Self-Assessment, schedule a Full User Security Assessment with the User Independent Security Assurance Service Provider; and

(c) within 12 months after each Full User Security Assessment, schedule a Verification User Security Assessment with the User Independent Security Assurance Service Provider.

G8.43 In assessing for the purposes of Sections G8.41 and G8.42 the number of Domestic Premises and Non-Domestic Premises supplied with electricity and/or gas through one or more Smart Metering Systems for which a User is the Responsible Supplier, that number shall, where any Shared Resources which are not provided by a Shared Resource Provider form part of both its User Systems and the User Systems of another User, be deemed to include any Domestic Premises or Non-Domestic Premises supplied with electricity and/or gas through one or more Smart Metering Systems for which that other User is the Responsible Supplier.

Network Parties

G8.44 Where a User is a Network Party and the number of Domestic Premises supplied with electricity and/or gas through one or more Smart Metering Systems for which it is the Electricity Distributor and/or the Gas Transporter exceeds 250,000, the User Security Assessment required by Section G8.40 shall be a Verification User Security Assessment and the User shall:

(a) within 12 months after previous Verification User Security Assessment, schedule a second Verification User Security Assessment with the User Independent Security Assurance Provider;

(b) within 12 months after each second successive Verification User Security Assessment, schedule a Full User Security Assessment with the User Independent Security Assurance Service Provider; and

(c) within 12 months after each Full User Security Assessment, schedule a Verification User Security Assessment with the User Independent Security Assurance Service Provider.

G8.45 Where a User is a Network Party and the number of Domestic Premises supplied with electricity and/or gas through one or more Smart Metering Systems for which it is the Electricity Distributor and/or the Gas Transporter is equal to or less than 250,000, the User Security Assessment required by Section G8.40 shall be a Verification User Security Assessment and the User shall:

(a) within 12 months after each Verification User Security Assessment, schedule a User Security Self-Assessment;

(b) within 12 months after each User Security Self-Assessment, schedule a Full User Security Assessment with the User Independent Security Assurance Service Provider; and

(c) within 12 months after each Full User Security Assessment, schedule a Verification User Security Assessment with the User Independent Security Assurance Service Provider.

G8.46 In assessing for the purposes of Sections G8.44 and G8.45 the number of Domestic Premises supplied with electricity and/or gas through one or more Smart Metering Systems for which a User is the Electricity Distributor and/or the Gas Transporter, that number shall, where any Shared Resources form part of both its User Systems and the User Systems of another User, be deemed to include any Domestic Premises supplied with electricity and/or gas through one or more Smart Metering Systems for which that other User is the Electricity Distributor and/or the Gas Transporter.

Other Users

G8.47 Where a User is neither a Supplier Party nor a Network Party, Section G8.40 requires the User to schedule a User Security Verification Assessment and the User shall:

(a) within 12 months after the previous User Security Verification Assessment, schedule a User Security Self-Assessment;

(b) within 12 months after the User Security Self-Assessment schedule a Full User Security Assessment with the User Independent Security Assurance Service Provider; and

(c) within 12 months after each Full User Security Assessment, schedule a User Security Verification Assessment.

Interpretation

G8.48 Section G8.49 applies where:

(a) pursuant to Sections G8.41 to G8.43, it is necessary to determine, in relation to any Supplier Party, the number of Domestic Premises and Non-Domestic Premises that are supplied with electricity and/or gas through one or more Smart Metering Systems for which it is the Responsible Supplier; or

(b) pursuant to Sections G8.44 to G8.46, it is necessary to determine, in relation to any Network Party, the number of Domestic Premises that are supplied with electricity and/or gas through one or more Smart Metering Systems for which it is the Electricity Distributor and/or the Gas Transporter.

G8.49 Where this Section applies:

(a) the determination referred to in Section G8.48 shall be made at the time at which the nature of each annual security assurance assessment for the relevant User falls to be ascertained; and

(b) the DCC shall provide all reasonable assistance that may be requested by that User or the Security Sub-Committee for the purposes of making that determination.

User Security Self-Assessment

G8.50 Where, in accordance with the requirements of this Section G8, a User is subject to a User Security Self-Assessment in any year, that User shall:

(a) carry out the User Security Self-Assessment during in accordance with the User Security Assessment Methodology that is applicable to User Security Self-Assessments; and

(b) ensure that the outcome of the User Security Self-Assessment is documented and is submitted to the User Independent Security Assurance Service Provider for review by no later than the date which is 12 months after the date of the completion of the previous User Security Assessment or (if more recent) User Security Self-Assessment.

Users: Obligation to Pay Explicit Charges

G8.51 Each User shall pay to the DCC all applicable Charges in respect of:

(a) all User Security Assessments and Follow-up Security Assessments carried out in relation to it by the User Independent Security Assurance Service Provider;

(b) the production by the User Independent Security Assurance Service Provider of any User Security Assessment Reports following such assessments; and

(c) all related activities of the User Independent Security Assurance Service Provider in respect of that User in accordance with this Section G8.

G8.52 Expenditure incurred in relation to Users in respect of the matters described in Section G8.51 shall be treated as Recoverable Costs in accordance with Section C8 (Panel Costs and Budgets).

G8.53 For the purposes of Section G8.51 the Panel shall, at such times and in respect of such periods as it may (following consultation with the DCC) consider appropriate, notify the DCC of:

(a) the expenditure incurred in respect of the matters described in Section G8.51 that is attributable to individual Users, in order to facilitate Explicit Charges designed to pass-through the expenditure to such Users pursuant to Section K7 (Determining Explicit Charges); and

(b) any expenditure incurred in respect of the matters described in Section G8.51 which cannot reasonably be attributed to an individual User.

Events of Default

G8.54 In relation to an Event of Default which consists of a material breach by a User of any of its obligations under Sections G3 to G6, the provisions of Sections M8.2 to M8.4 shall apply subject to the provisions of Sections G8.55 to G8.60.

G8.55 Where in accordance with Section M8.2 the Panel receives notification that a User is in material breach of any requirements of Sections G3 to G6, it shall refer the matter to the Security Sub-Committee.

G8.56 On any such referral the Security Sub-Committee may investigate the matter in accordance with Section M8.3 as if the references in that Section to the “Panel” were to the “Security Sub-Committee”.

G8.57 Where the Security Sub-Committee has:

(a) carried out an investigation in accordance with Section M8.3; or

(b) received a report from the User Independent Security Assurance Service Provider, following a User Security Assessment, concluding that a User is in actual or potential non-compliance with any of its obligations under Sections G3 to G6,

the Security Sub-Committee shall consider the information available to it and, where it considers that actual non-compliance with any obligations under Sections G3 to G6 has occurred, shall refer the matter to the Panel for it to determine whether that non- compliance constitutes an Event of Default.

G8.58 Where the Panel determines that an Event of Default has occurred, it shall:

(a) notify the relevant User and any other Party it considers may have been affected by the Event of Default; and

(b) determine the appropriate steps to take in accordance with Section M8.4.

G8.59 Where the Panel is considering what steps to take in accordance with Section M8.4, it may request and consider the advice of the Security Sub-Committee.

G8.60 Where the Panel determines that a User is required to give effect to a remedial action plan in accordance with Section M8.4(d) that plan must be approved by the Panel (having regard to any advice of the Security Sub-Committee).

Shared Resource Providers

G8.61 Section G8.62 applies where:

(a) Shared Resources are provided to a User by a Shared Resource Provider; and

(b) any User Security Assessment is carried out in respect of that Shared Resource Provider.

G8.62 Where this Section applies:

(a) the outcome of the User Security Assessment (including for these purposes any actions or decisions described at Sections G8.22 to G8.29) shall be treated as applying to the User, in respect of the Shared Resources, in the same manner as it is applicable to the Shared Resource Provider; and

(b) in any User Security Assessment which takes place in respect of the User, the User Independent Security Assessment Service Provider shall, with regard to matters relating to the Shared Resources, rely on the outcome of the most recent User Security Assessment in respect of the Shared Resource Provider and shall not be required to repeat that assessment.

G8.63 For the purposes of Section G8.40, where a Shared Resource Provider provides Shared Resources to Users which are:

(a) Supplier Parties, the provisions of Sections G8.41 and G8.42 shall apply to the Shared Resource Provider as if it was a Supplier Party and the Smart Metering Systems for which those Supplier Parties are the Responsible Suppliers were Smart Metering Systems for which it is the Responsible Supplier;

(b) Network Parties, the provisions of Sections G8.44 to G8.46 shall apply to the Shared Resource Provider as if it was a Network Party and the Smart Metering Systems for which those Network Parties are the Electricity Distributor and/or Gas Transporter were Smart Metering Systems for which it is the Electricity Distributor and/or Gas Transporter;

(c) Other Users, the provisions of Section G8.47 shall apply to the Shared Resource Provider as if it was an Other User.

CPA Certificate Remedial Plan Preparation

G8.64 Where a User is a Supplier Party, the User shall ensure that it has in place (and periodically reviews) a policy for creating and managing compliance with CPA Certificate Remedial Plans.

G9. DCC SECURITY ASSURANCE

The DCC Independent Security Assessment Arrangements

G9.1 The DCC shall establish, give effect to, maintain and comply with arrangements, to be known as the " **DCC Independent Security Assessment Arrangements**", which shall procure the services of a DCC Independent Security Assessment Service Provider to undertake security assessment services.

Scope of Security Assessment Services

G9.2 The security assessment services specified in this Section G9.2 are services in accordance with which the DCC Independent Security Assessment Service Provider shall:

(a) carry out DCC Security Assessments at such times and in such manner as is provided for in this Section G9;

(b) produce DCC Security Assessment Reports in relation to the DCC that have been the subject of a DCC Security Assessment;

(c) receive, consider and validate DCC Security Assessment Responses and carry out any Follow-up Security Assessments at the request of the Security Sub-Committee;

(d) otherwise, at the request of, and to an extent determined by, the Security Sub Committee, carry out an assessment of the compliance of the DCC with its obligations under:

(i) Condition 8 (Security Controls for the Authorised Business) of the DCC Licence;

(ii) the requirements of Sections G2 and G4 to G6 or any CPA Certificate Remedial Plan; and where:

(iii) following either a DCC Security Assessment, any material increase in the security risk relating to the DCC has been identified; or

(iv) the Security Sub-Committee otherwise considers it appropriate for that assessment to be carried out;

(e) at the request of the Security Sub-Committee, provide to it advice in relation to:

(i) the compliance of the DCC with its obligations under SEC Section G or any CPA Certificate Remedial Plan; and

(ii) changes in security risks relating to the Systems, Data, functionality and processes of the DCC which fall within SEC Section G5 (Information Security: Obligations on the DCC);

(f) at the request of the Security Sub-Committee, provide to it advice in relation to the suitability of any remedial action plan for the purposes of Section M8.4 of the Code (Consequences of an Event of Default);

(g) at the request of the Security Sub-Committee Chair, provide a representative to attend and contribute to the discussion at any meeting of the Security Sub-Committee; and

(i) undertake such other activities and do so at such times and in such manner, as may be further provided for in this Section G9;

(ii) assess the DCC's compliance with the requirements of Condition 8 (Security Controls for the Authorised Business) of the DCC Licence;

(iii) such other requirements relating to the security of the DCC Total System as may be specified by the Security Sub-Committee or the Panel from time to time.

G9.3 The actions specified in this Section G9.3 shall be actions taken by the DCC to:

(a) procure the provision of security assessment services by the DCC Independent Security Assessment Service Provider (as further described in Section G9.4);

(b) ensure that the DCC Independent Security Assessment Service Provider carries out Security Assessments for the purpose specified in Section G9.2:

(i) annually;

(ii) on any material change to the DCC Total System; and

(iii) at any other time specified by the Security Sub-Committee or the Panel;

(c) comply with the arrangements set out by the Security Sub-Committee in a Security Controls Framework;

(d) in line with the methodology and processes set out in the Security Controls Framework:

(i) procure that the DCC Independent Security Assessment Service Provider produces a DCC Security Assessment Report following each such assessment that has been carried out;

(ii) ensure that the DCC Independent Security Assessment Service Provider provides the Security Sub-Committee with a copy of each such DCC Security Assessment Report;

(iii) produce a DCC Security Assessment Response in relation to each such report; and

(iv) provide to the Panel and the Security Sub-Committee a copy of each DCC Security Assessment Response and, as soon as reasonably practicable thereafter, a report on its implementation of any action plan that is required by the Security Sub-Committee.

The DCC Independent Security Assessment Service Provider

G9.4 For the purposes of Section G9.3, the "**DCC Independent Security Assessment Service Provider**" shall be a person who is appointed by the DCC to provide security assessment services:

(a) of the scope specified in Section G9.2;

(b) from a person who:

(i) is suitably qualified in accordance with Section G9.5;

(ii) is suitably independent in accordance with Section G9.8.

Suitably Qualified Service Provider

G9.5 The DCC Independent Security Assessment Service Provider shall be treated as suitably qualified in accordance with this Section G9.5 only if it satisfies:

(a) the requirements specified in Section G9.6; and

(b) the requirement specified in Section G9.7.

G9.6 The requirements specified in this Section G9.6 are that the DCC Independent Security Assessment Service Provider:

(a) is accredited by UKAS as meeting the requirements for providing audit and certification of information security management systems in accordance with ISO/IEC 27001:2017 Information Technology – Security Techniques – Information Security Management Systems) or any equivalent to that standard which updates or replaces it from time to time; and/or

(b) holds another membership, accreditation, approval or form of professional validation that is in the opinion of the Security Sub-Committee substantially equivalent in status and effect to the arrangements described in paragraph (a).

G9.7 The requirement specified in this Section G9.7 is that the DCC Independent Security Assessment Service Provider:

(a) employs consultants who are assured under an official cyber security qualification scheme recognised by NCSC or the UK Cyber Security Council or UKAS and which is approved by the Security Sub-Committee at levels equivalent to 'Chartered', 'Principal', 'Lead' or 'Senior Practitioner' in either 'Security and Information Risk Advisor' or 'Information Assurance Auditor' roles; and

(b) engages those individuals as its lead auditors for the purposes of carrying out all security assessments in accordance with this Section G7.

Independence Requirement

G9.8 The DCC Independent Security Assurance Service Provider shall be treated as suitably independent in accordance with this Section G9.8 only if it satisfies:

(a) the requirements specified in Section G9.9; and

(b) the requirement specified in Section G9.10.

G9.9 For the purposes of Sections G9.9 and G9.10:

(a) the DCC must be independent from the DCC Independent Security Assessment Service Provider in carrying out functions under this Section G9; and

(b) all of the DCC's Service Providers must be independent from the DCC Independent Security Assessment Service Provider in carrying out its functions to assess the DCC's compliance with its obligations as the DCC under Sections G2 and G4 to G6 and DCC Licence Condition 8 (Security Controls for the Authorised Business) and SEC Appendix Z Sections 6 and 7.

G9.10 The requirements specified in this Section G9.10 are that:

(a) neither the DCC or any of its subsidiaries, and no DCC Service Provider or any of its subsidiaries, holds or acquires any investment by way of shares, securities or other financial rights or interests in the DCC Independent Security Assessment Service Provider;

(b) no director of the DCC and no director of any DCC Service Provider, is or becomes a director or employee of, or holds or acquires any investment by way of shares, securities or other financial rights or interests in, the DCC Independent Security Assessment Service Provider; and

(c) the DCC Independent Security Assessment Service Provider does not hold or acquire a participating interest (as defined in section 421A of the Financial Services and Markets Act 2000) in the DCC or any of the DCC's Service Providers, (for these purposes references to the DCC's Service Providers shall not include the DCC Independent Security Assessment Service Provider where it acts in that capacity).

G9.11 The requirement specified in this Section G9.11 is that the DCC Independent Security Assessment Service Provider is able to demonstrate to the satisfaction of the Security Sub-Committee that it has in place arrangements to ensure that it will at all times act independently of any commercial relationship that it has, has had, or may in future have with the DCC or the DCC's Service Providers (and for these purpose a 'commercial relationship' shall include a relationship established by virtue of the DCC Independent Security Assessment Service Provider itself being a DCC Service Provider to the DCC).

Compliance of the DCC Independent Security Assessment Service Provider

G9.12 The Security Sub-Committee shall advise the DCC of any performance failures or non-compliance with the SEC obligations on the part of the DCC Independent Security Assessment Service Provider to enable the DCC to ensure that the DCC Independent Security Assessment Service Provider carries out its functions in accordance with the provisions of this Section G12.

DCC: Duty to Cooperate in Assessment

G9.13 The DCC shall do all such things as may be reasonably requested by the Security Sub- Committee, or by any person acting on behalf of or at the request of the Security Sub- Committee (including in particular the DCC Independent Security Assessment Service Provider), for the purposes of facilitating an assessment of the DCC's compliance with its obligations under Sections G2 and G4 to G6 or DCC Licence Condition 8 (Security Controls for the Authorised Business) or SEC Appendix Z Sections 6 and 7 and any CPA Certificate Remedial Plan.

G9.14 For the purposes of Section G9.13, the DCC shall provide the DCC Independent Security Assessment Service Provider with:

(a) all such Data as may reasonably be requested, within such times and in such format as may reasonably be specified;

(b) all such other forms of cooperation as may reasonably be requested, including in particular:

(i) access at all reasonable times to such parts of the premises of the DCC or its Service Providers as are used for, and such persons engaged by the DCC as carry out or are authorised to carry out, any activities related to its compliance with its obligations under Sections G2 and G4 to G6 and DCC Licence Condition 8 (Security Controls for the Authorised Business) and SEC Appendix Z Sections 6 and 7; and

(ii) such cooperation as may reasonably be requested by the DCC Independent Security Assessment Services Provider for the purposes of carrying out any security assurance assessment in accordance with this Section G9.

Categories of DCC Security Assessment

G9.15 For the purposes of this Section G9, there shall be the following two categories of security assessment:

(a) a Full DCC Security Assessment (as further described in Section G9.16);

(b) a Follow-up DCC Security Assessment (as further described in Section G9.17).

G9.16 A "**Full DCC Security Assessment**" shall be an assessment carried out by the DCC Independent Security Assessment Service Provider in respect of the DCC and its Service Providers to identify the extent to which the DCC is compliant with each of its obligations under Sections G2 and G4 to G6 and DCC Licence Condition 8 (Security Controls for the Authorised Business) and SEC Appendix Z Sections 6 and 7.

G9.17 A "**Follow-up DCC Security Assessment**" shall be an assessment carried out by the DCC Independent Security Assessment Service Provider, following a DCC Security Assessment, in accordance with the provisions of Section G9.25.

DCC Security Assessments: General Procedure

DCC Security Assessment Methodology

G9.18 Each DCC Security Assessment carried out by the DCC Independent Security Assessment Service Provider shall be carried out in accordance with the Security Controls Framework developed as defined in G7.19(a).

The DCC Security Assessment Report

G9.19 Following the completion of a DCC Security Assessment, the DCC Independent Security Assessment Service Provider shall, in discussion with the DCC, produce a written report (a "**DCC Security Assessment Report**") which shall:

(a) set out the findings of the DCC Independent Security Assessment Service Provider on all the matters within the scope of the DCC Security Assessment;

(b) specify any instances of actual or potential non-compliance of the DCC with its obligations under Sections G2 and G4 to G6 which have been identified by the DCC Independent Security Assessment Service Provider;

(c) specify any instances of actual or potential non-compliance of the DCC with its obligations under DCC Licence Condition 8 (Security Controls for the Authorised Business);

(d) specify any instances of actual or potential non-compliance of the DCC with its obligations under SEC Appendix Z, Sections 6 and 7; and

(e) set out the evidence which, in the opinion of the DCC Independent Security Assessment Service Provider, establishes each of the instances of actual or potential non-compliance which it has identified.

G9.20 The DCC Independent Security Assessment Service Provider shall submit a copy of each DCC Security Assessment Report to the Security Sub-Committee and to the DCC.

The DCC Security Assessment Response

G9.21 Following the receipt by the DCC of a DCC Security Assessment Report which relates to it, the DCC shall as soon as reasonably practicable, and in any event by no later than such date as the Security Sub-Committee may specify:

(a) produce a written response to that report (a "**DCC Security Assessment Response**") which addresses the findings set out in the report; and

(b) submit a copy of that response to the Security Sub-Committee and the DCC Independent Security Assessment Service Provider.

G9.22 Where a DCC Security Assessment Report following a Full DCC Security Assessment, specifies any instance of actual or potential non-compliance of the DCC with its obligations under Sections G2 and G4 to G6 and/or with DCC Licence Condition 8 (Security Controls for the Authorised Business) and/or with SEC Appendix Z, Sections 6 and 7, the DCC shall ensure that its DCC Security Assessment response includes the matters referred to in Section G9.23.

G9.23 The matters referred to in this Section are that the DCC Security Assessment Response:

(a) indicates whether the DCC accepts the relevant findings of the DCC Independent Security Assessment Service Provider and, where it does not, explains why this is the case;

(b) sets out any steps that the DCC has taken or proposes to take in order to remedy and/or mitigate the actual or potential non-compliance or the increase in security risk (as the case may be) specified in the DCC Security Assessment Report; and

(c) identifies a timetable within which the DCC proposes to take any such steps that have not already been taken.

G9.24 Where a DCC Security Assessment Response sets out any steps that the DCC proposes to take in accordance with Section G9.23(b), the Security Sub-Committee (having considered the advice of the DCC Independent Security Assessment Service Provider) shall review that response and either:

(a) notify the DCC that it accepts that the steps that the DCC proposes to take, and the timetable within which it proposes to take them, are appropriate to remedy and/or mitigate the actual or potential non-compliance or increase in security risk (as the case may be) specified in the DCC Security Assessment Report; or

(b) seek to agree with the DCC such alternative steps and/or timetable as would, in the opinion of the Security Sub-Committee, be more appropriate for that purpose.

G9.25 Where a DCC Security Assessment Response sets out any steps that the DCC proposes to take in accordance with Section G9.23(b), and where those steps and the timetable within which it proposes to take them are accepted by the Security Sub-Committee, or alternative steps and/or an alternative timetable are agreed between it and the DCC in accordance with Section G9.24(b), the DCC shall:

(a) take the steps that have been accepted or agreed (as the case may be) within the timetable that has been accepted or agreed (as the case may be); and

(b) report to the Security Sub-Committee on:

(i) its progress in taking those steps, at any such intervals or by any such dates as the Security Sub-Committee may specify;

(ii) the completion of those steps in accordance with the timetable; and

(iii) any failure to complete any of those steps in accordance with the timetable, specifying the reasons for that failure.

Follow-up Security Assessment

G9.26 Where a DCC Security Assessment Response sets out any steps that the User proposes to take in accordance with Section G9.23(b), and where those steps and the timetable within which it proposes to take them are accepted by the Security Sub-Committee, or alternative steps and/or an alternative timetable are agreed between it and the User in accordance with Section G9.24(b), the DCC Independent Security Assessment Service Provider shall, at the request of the Security Sub-Committee (and by such date as it may specify), carry out a Follow-up Security Assessment of the DCC to:

(a) identify the extent to which the DCC has taken the steps that have been accepted or agreed (as the case may be) within the timetable that has been accepted or agreed (as the case may be); and

(b) assess any other matters related to the DCC Security Assessment Response that are specified by the Security Sub-Committee.

DCC Security Assessments: Further Provisions

G9.27 The DCC Independent Security Assessment Service Provider may, in carrying out any DCC Security Assessment, take into account any relevant security accreditation or certification held by the DCC.

Setting the Compliance Status

G9.28 Following the completion of a Full DCC Security Assessment, the Security Sub-Committee shall consider the DCC Security Assessment Report and the DCC Security Assessment Response.

G9.29 The Security Sub-Committee shall identify whether any remaining non-compliances that exist with Section G2 or G4 to G6 and/or the DCC Licence Condition 8 (Security Controls for the Authorised Business) and/or SEC Appendix Z, Sections 6 and 7 and shall, where appropriate:

(a) note and record that there are no non-compliances; or

(b) note and record the specific non-compliances that need to be addressed.

G9.30 Where the Security Sub-Committee identifies remaining non-compliances that exist with Section G2 and G4 to G6 and/or the DCC Licence Condition 8 (Security Controls for the Authorised Business) and/or SEC Appendix Z Sections 6 and 7, it shall:

(a) require the DCC to take the steps set out in Section G9.24: or

(b) require a Follow-up Security Assessment as set out in Section G9.26.

G9.31 Where the Security Sub-Committee identifies any remaining non-compliances with Section G2 or G4 to G6 and/or the DCC Licence Condition 8 (Security Controls for the Authorised Business) and/or SEC Appendix Z, Sections 6 and 7, it shall notify the Panel as required by G9.37(b).

CPA Certificate Remedial Plan Preparation

G9.32 The DCC shall ensure that it has in place (and periodically reviews) a policy for creating and managing compliance with CPA Certificate Remedial Plans. The DCC Independent Security Assessment Service Provider will assess the DCC's compliance with Appendix Z Section 6 and Section 7.

Disagreement with Security Sub-Committee Decisions

G9.33 Where the DCC disagrees with any decision made by the Security Sub-Committee in relation to it under Section G9.28 to G9.31, it may appeal that decision to the Panel. If the DCC disagrees with any decision made by the Panel, it may appeal that decision to the Authority and the determination of the Authority shall be final and binding for the purposes of the Code.

Events of Default

G9.34 In relation to an Event of Default which consists of a material breach by the DCC of any of the obligations referred to at Section G9.2(c), the provisions of Sections M8.2 to M8.4 shall apply subject to the provisions of Sections G9.35 to G9.41.

G9.35 For the purposes of Sections M8.2 to M8.4 as they apply pursuant to Section G9.34, an Event of Default shall (notwithstanding the ordinary definition thereof) be deemed to have occurred in respect of the DCC where it is in material breach of any of the obligations referred to at Section G9.2(d) (provided that Sections M8.4(e), (f) and (g) shall never apply to the DCC).

G9.36 Where in accordance with Section M8.2 the Panel receives notification that the DCC is in material breach of any of the obligations referred to at Section G9.2(d), it shall refer the matter to the Security Sub-Committee.

G9.37 On any such referral the Security Sub-Committee may investigate the matter in accordance with Section M8.3 as if the references in that Section to the "Panel" were to the "Security Sub-Committee".

G9.38 Where the Security Sub-Committee has:

(a) carried out an investigation in accordance with Section M8.3; or

(b) received a DCC Security Assessment Report concluding that the DCC is in actual or potential non-compliance with any of the obligations referred to at Section G9.2(c),

the Security Sub-Committee shall consider the information available to it and, where it considers that actual non-compliance with any of the obligations referred to at Section G9.2(c) has occurred, shall refer the matter to the Panel for it to determine whether that non-compliance constitutes an Event of Default.

G9.39 Where the Panel determines that an Event of Default has occurred, it shall:

(a) notify the DCC and any other Party it considers may have been affected by the Event of Default; and

(b) determine the appropriate steps to take in accordance with Section M8.4.

G9.40 Where the Panel is considering what steps to take in accordance with Section M8.4, it may request and consider the advice of the Security Sub-Committee.

G9.41 Where the Panel determines that the DCC is required to give effect to a remedial action plan in accordance with Section M8.4(d) that plan must be approved by the Panel (having regard to any advice of the Security Sub-Committee).

CPA Certificate Remedial Plan Preparation

G9.42 The DCC shall ensure that it has in place (and periodically reviews) a policy for creating and managing compliance with CPA Certificate Remedial Plans.

G10. SHARED RESOURCES

G10.1 Where any resources which form part of the User Systems of a User also form part of the User Systems of any one or more other Users, those resources shall be known as "**Shared Resources**".

G10.2 For the purposes of this Part G, a "**Shared Resource Provider**" shall mean any Party which makes available Shared Resources to one or more Users, for use by them or on their behalf, in accordance with any agreement entered into or arrangement made with each such User.

Shared Resources which constitute the entirety of User Systems

G10.3 A User may not employ Shared Resources which:

(a) are made available to it by one other person; and

(b) constitute the entirety of its User Systems,

unless those Shared Resources are provided by a Shared Resource Provider.

Obligations on Shared Resource Providers

G10.4 Each Shared Resource Provider shall:

(a) maintain a list of every User to which it makes available Shared Resources in accordance with an agreement or arrangement of the type described in Section G10.2;

(b) revise that list from time to time to ensure that it remains accurate and up to date at all times;

(c) submit to the Security Sub-Committee a copy of that list and of any revision to it, so that the Security Sub-Committee is in possession of a copy of that list that is accurate and up to date at all times.

G10.5 For the purposes of Sections G1 to G5 and G7 to G9, unless the context otherwise requires, a Shared Resource Provider shall be treated as if it were a User, and:

(a) any reference to a User shall be deemed to include a reference to that Shared Resource Provider;

(b) subject to Section G10.6, obligations in those Sections which are expressed to apply to a User shall apply to that Shared Resource Provider;

(c) references in those obligations to User Systems shall be deemed, for the purpose of their application to the Shared Resource Provider, to be references to the Shared Resources which it provides; and

(d) the role of the Shared Resource Provider shall be treated as if it were an additional category of User Role.

Continuing Obligations of Users

G10.6 Section G10.5 shall have effect without prejudice to the duty of Users to comply with the obligations at Sections G1 to G5 and G7 to G9, so that, where a Shared Resource Provider provides a User with Shared Resources constituting its User Systems, both it and the User shall be jointly and severally liable for any failure to comply with an obligation which relates to those Shared Resources, subject to:

(a) Section G5.28 which has effect for determining the obligations of, and the relationship between, the User and the Shared Resource Provider in relation to their respective User Information Security Management Systems; and

(b) Sections G8.61 to G8.63 which have effect for determining:

(i) when the Shared Resource Provider is required to schedule either a User Security Assessment or User Security Self-Assessment; and

(ii) how the outcome of a User Security Assessment in respect of the Shared Resource Provider is applicable to a User to which that Shared Resource Provider is providing Shared Resources.

Additional Obligations following User Security Assessments

G10.7 Section G10.8 applies, following a User Security Assessment that has been carried out in respect of a Shared Resource Provider, in relation to the information to be provided to each User with which, at that time, the Shared Resource Provider has an agreement or arrangement of the type described in Section G10.2 (a "**Shared Resource User**").

G10.8 Where this paragraph applies:

(a) the User Independent Security Assurance Service Provider shall (in addition to its obligation at Section G8.23) submit a copy of the User Security Assessment Report to each Shared Resource User;

(b) the Shared Resource Provider shall (in addition to its obligation at Section G8.24) submit a copy of its User Security Assessment Response to each Shared Resource User;

(c) the Security Sub-Committee shall (in addition to its obligation at Section G8.27) notify each Shared Resource User of any steps accepted or agreed (as the case may be) with the Shared Resource Provider; and

(d) the Shared Resource Provider shall (in addition to its obligation at Section G8.28(b)) provide each Shared Resource User with a copy of any report that is submitted from time to time to the Security Sub-Committee in accordance with Section G8.28(b).

Interpretation

G10.9 For the purposes of Sections G1 to G5 and G7 to G9, unless the context otherwise requires, any expressions which are:

(a) defined in those Sections by reference to a User or User Systems; or

(b) defined in Section A by reference to a User or User Systems, and used in those Sections,

shall be interpreted so that any reference to a User is deemed to include a reference to a Shared Resource Provider, and any reference to User Systems is deemed, in the case of a Shared Resource Provider, to be a reference to the Shared Resources provided by it.

G11. THE ECOS TRANSITION AND MIGRATION APPROACH DOCUMENT

Overview

G11.1 The first version of the ECoS Transition and Migration Approach Document is to be developed by the Secretary of State and incorporated into this Code pursuant to Part G of Condition 22 of the DCC Licence and Section X5 (Incorporation of Certain Documents into this Code).

G11.2 The second (and each subsequent version as may be required) of the ECoS Transition and Migration Approach Document is to be developed by the DCC pursuant to this Section G11, and incorporated into this Code pursuant to Part G of Condition 22 of the DCC Licence and, where Section X continues to be in effect, Section X5 (Incorporation of Certain Documents into this Code).

Purpose of the ECoS Transition and Migration Approach Document

G11.3 The purpose of the first version of the ECoS Transition and Migration Approach Document is to provide that the modifications made to this Section G and to Section L of the Code for the purposes of setting out the arrangements which are to apply following the completion of ECoS Migration, shall not apply in respect of any period which is prior to:

(a) the commencement of ECoS Migration; and

(b) the point in time at which Devices with Device Security Credentials that comprise (in part) information from an ECoS Certificate may be Commissioned.

G11.4 In addition to the purpose set out in Section G11.3, the purposes of the second (and each subsequent) version of the ECoS Transition and Migration Approach Document are to:

(a) enable the ECoS Migration of SMETS2+ Devices such that the Device Security Credentials for such Devices comprise (in part) information from an ECoS Certificate instead of information from a TCoS Certificate;

(b) facilitate the processing of a 'CoS Update Security Credentials' Service Request made by the TCoS Service Provider in respect of any Device that has not ECoS Migrated;

(c) permit, for a transitional period, the installation of Devices in respect of which the Device Security Credentials are comprised (in part) by information from a TCoS Certificate;

(d) provide for additional and/or varied provisions to apply for a transitional period prior to, during and/or following the ECoS Migration of Devices; and

(e) provide for additional and/or varied provisions to apply for a transitional period to manage the interactions between the Enduring Change of Supplier Arrangements and the introduction of the

Centralised Registration Service, which may take place prior to, during, or following the commencement of ECoS Migration.

Content of the ECoS Transition and Migration Approach Document

G11.5 The ECoS Transition and Migration Approach Document may include, without limitation, some or all of the following:

(a) rights and/or obligations of the DCC and other Parties designed to facilitate or achieve the purposes of the ECoS Transition and Migration Approach Document which are either additional to or vary other rights and/or obligations set out in this Code;

(b) the processes by which SMETS2+ Devices that have been Commissioned will have their Device Security Credentials updated such that those security credentials which relate to the CoS Party will be derived from information contained in an ECoS Certificate instead of information contained in a TCoS Certificate;

(c) the processes by which changes to DCC Systems are to be made to enable the DCC to begin processing "CoS Update Security Credentials" Service Requests in relation to SMETS1 Devices;

(d) pre-conditions to apply in relation to the ECoS Migration of any SMETS1 or SMETS2+ Device, including by reference to the DCC, the Device Model, and/or the Responsible Supplier;

(e) provisions enabling the DCC to process a 'CoS Update Security Credentials' Service Request in a different way, method or manner depending upon whether or not the Device in respect of which the Service Request is made has been ECoS Migrated;

(f) provisions that, from any such date as may be specified, permit or require any newly installed or Commissioned Device to have security credentials which relate to the CoS Party to be derived from the information contained in an ECoS Certificate instead of information that is contained in a TCoS Certificate;

(g) provisions requiring the DCC to report on its progress on ECoS Migration, including identifying whether in relation to Devices any particular category of Device Model and/or Device Type has failed, or is more likely to fail, ECoS Migration;

(h) provisions requiring the DCC to apply a specific strategy in respect of attempting to complete ECoS Migration for a Device in respect of which ECoS Migration has previously failed;

(i) provisions requiring the DCC and Supplier Parties to take steps to resolve matters that are causing, or contributing to the cause of, failures of ECoS Migration;

(j) provisions requiring the secure decommissioning of Systems of the TCoS Service Provider, for the revocation of any associated Organisation Certificates, and for the verifiable destruction of associated Private Keys;

(k) limitations and/or variations to the Services and/or the rights and/or obligations of the Parties to apply for a transitional period prior to and/or following the ECoS Migration of some or all Devices, which may include limitations and/or variations to Services in light of other proposed changes to this Code; and

(l) provision for the referral and determination of disputes in respect of the ECoS Transition and Migration Approach Document, which may include interim or final determinations by the Secretary of State, the Authority, the Panel or any other person specified by the Secretary of State.

Process to Develop Second (and any subsequent) Document for Designation

G11.6 The DCC shall, where so directed by the Secretary of State from time to time, develop and consult upon the second (and any subsequent) version of the ECoS Transition and Migration Approach Document and submit it to the Secretary of State in accordance with the following process:

(a) the DCC shall, in consultation with the Parties, such other persons as are likely to be interested, and where Section G11.7 applies, the Security Sub-Committee, produce a draft of the document;

(b) where a disagreement arises with any Party or other person with regard to any proposal as to the content of the document, the DCC shall endeavour to reach an agreed proposal with that person consistent with the purposes of the ECoS Transition and Migration Approach Document;

(c) the DCC shall send a copy of the draft document to the Secretary of State as soon as is practicable after completion of the process described in paragraphs (a) and (b) above, and shall when doing so provide to the Secretary of State:

(i) a statement of the reasons why the DCC considers that draft to be fit for purpose;

(ii) copies of the consultation responses received; and

(iii) a summary of any disagreements that arose during consultation and that have not been resolved by reaching an agreed proposal;

G11.7 Where the DCC reasonably believes that any changes to a version of the ECoS Transition and Migration Approach Document it is developing in accordance with Section G11.6 might be considered to have an impact upon on the End-to-End Security Architecture or the risks identified in the Security Risk Assessment:

(a) the DCC shall submit to the Security Sub-Committee for its review and comment an impact assessment that sets out the DCC's views of any such impact (a **Security Impact Assessment**);

(b) the Security Sub-Committee shall provide any comments or observations that they have on the Security Impact Assessment to the DCC;

(c) the DCC shall provide a response to any such comments or observations to the Security Sub-Committee and update the relevant draft of the ECoS Transition and Migration Approach Document as appropriate to take into account the comments or observations; and

(d) following the DCC's response, the Security Sub-Committee shall notify the Secretary of State whether it considers there to be any remaining outstanding unacceptable risks to the End-to-End Security Architecture as a consequence of the proposed changes to the ECoS Transition and Migration Approach Document.

G11.8 The DCC shall comply with any direction given to it by the Secretary of State following the Secretary of State's consideration of the draft document which direction may require the DCC to:

(a) make such amendments to the draft document as are set out or described in the direction;

(b) produce and submit to the Secretary of State a further draft of the document; and

(c) follow a specified process (and the time within which that process shall be completed) prior to submitting a further draft of the document to the Secretary of State.

Application of the ECoS Transition and Migration Approach Document

G11.9 The DCC and the categories of Party referred to in the ECoS Transition and Migration Approach Document shall comply with the ECoS Transition and Migration Approach Document.

G11.10 The ECoS Transition and Migration Approach Document shall have priority over the other SEC Subsidiary Documents in relation to the subject matter of the ECoS Transition and Migration Approach Document.

Expiry of each version of the ECoS Transition and Migration Approach Document

G11.11 The second, and each subsequent, version of the ECoS Transition and Migration Approach Document shall provide for a date (or a mechanism for determining a date) from which that version is to no longer apply. From such date, that version of the ECoS Transition and Migration Approach Document shall no longer have any effect (but without prejudice to the rights and obligations arising prior to that date) and it shall automatically be deleted from this Code.

Definitions

G11.12 For the purposes of this Section G11:

Centralised Registration Service	has the meaning given to that term in Condition 1 of the DCC Licence.
ECoS Certificate	means an Organisation Certificate for which the ECoS Service Provider is the Subject.
ECoS Migration	means, in relation to any one or more Device(s), that the Device Security Credentials held on or in relation to any such Device previously populated with information from a TCoS Certificate have been populated with information from an ECoS Certificate, and the expression "**ECoS Migrated**" shall be interpreted accordingly.
ECoS Service Provider	means each DCC Service Provider that, following the completion of the implementation of the Enduring Change of Supplier Arrangements, supports or is to support the performance of tasks ascribed to the CoS Party.
Enduring Change of Supplier Arrangements	has the meaning given to that term in Condition 13A of the DCC Licence.
Subject	has the meaning given to that term in Annex A of Appendix B (Organisation Certificate Policy).
TCoS Certificate	means an Organisation Certificate for which the TCoS Service Provider is the Subject.

TCoS Service Provider	means the DCC Service Provider that, prior to the commencement of the implementation of the Enduring Change of Supplier Arrangements, is the service provider that supports the performance of tasks ascribed to the CoS Party.

G12. SECURITY ASSURANCE OF DEVICE TRIAGE FACILITIES

G12.1 Some of the expressions used in this Section G12 are defined in Section G12.9.

G12.2 Where the SSC Guidance for Device Security Assurance and Triage specifies that independent assurance of Triage Facility Providers is required to achieve appropriate levels of security assurance in accordance with the requirements of this Code, this Section G12 shall apply.

Triage Facility Provider Obligations

G12.3 In order to become a Triage Facility Provider, an entity must either be an existing Party or accede to this Code and become a Party. A Triage Service Provider is not required to be a User.

G12.4 Each Triage Facility Provider shall:

(a) not attempt to undertake Triage Activities on any Device where the tamper-protection boundary required by the CPA Security Characteristics has already been breached before reaching the Triage Facility (taking into account any allowable breaches necessary as part of essential Device maintenance and/or the de-commissioning process);

(b) only use the Triage Tool and Triage System Interface provided by a Device's Manufacturer to access the Manufacturer's Triage System and not use any other electronic devices, interfaces or IT systems for carrying out Triage Activities;

(c) ensure multi-factor authentication and role-based access controls are used within its Triage Facility to control access to the graphical user interface (GUI) of the Triage Tool, and to control access to the Triage System Interface;

(d) at all times prevent unauthorised use of the Triage Tool and Triage System Interface, and ensure the physical security of the Triage Tool and any Devices that are subject to Triage Activities;

(e) ensure that all the required tamper-protection seals are fitted to Devices on completing the Triage Activities;

(f) maintain an asset management system to record Triage Activities undertaken at the Triage Provider's Triage Facility, including details of:

(i) the Requestor of any change to the configuration of a Device;

(ii) the Device Model and serial number of each Device where the tamper-protection boundary is breached in order to undertake (or attempt to undertake) Triage Activities;

(iii) details of Triage Activities successfully undertaken;

(iv) details of any failed attempts to complete Triage Activities; and

(v) confirmation that any seals and tamper-protection required by the CPA Security Characteristics have been applied before returning a Device to a Requestor.

(g) when requested by the Security Sub-Committee, provide the Security Sub-Committee with an up-to-date copy of the records maintained pursuant to Section G12.3(f);

(h) provide all reasonable assistance that may be requested by the Security Sub-Committee or the User Independent Security Assurance Service Provider for the purposes of conducting a User Security Assessment;

(i) subject to Section G12.5, comply with the requirements of Sections G1, G3 to G5, G7 and G8;

(j) comply with the requirements of Sections G12.6 to G12.8; and

(k) act in accordance with Good Industry Practice.

G12.5 For the purposes of Sections G1, G3 to G5, G7 and G8, unless the SSC Guidance for Device Security Assurance and Triage states otherwise, a Triage Facility Provider shall be treated as if it is a User and:

(a) any reference to a 'User' shall be deemed to include a reference to a 'Triage Facility Provider';

(b) except for where the SSC Guidance for Device Security Assurance and Triage states otherwise, obligations in those Sections which are expressed to apply to a User shall apply to a Triage Facility Provider;

(c) references in those obligations to 'User Systems' shall be deemed, for the purpose of their application to the Triage Facility Provider, to be references to the Triage Activities undertaken at the Triage Facility; and

(d) the Security Sub-Committee shall provide Triage Facility Providers and other Parties with guidance on interpretation of Sections G1, G3 to G5, G7 and G8 in respect of their application to Triage Facility Providers and Triage Activities.

User Security Assessments of Triage Facilities

G12.6 Prior to undertaking any Triage Activities, each Triage Facility Provider shall be subject to an initial Full User Security Assessment by a User Independent Security Assurance Service Provider following the process in Sections G8.22 to G8.30.

Approval

G12.7 On receipt of the initial Full User Security Assessment Report and the User Security Assessment Response, the assurance status shall be set in accordance with Sections G8.35 to G8.36 and:

(a) where the assurance status is set to ‘approved' under Section G8.36(a) then the Triage Facility Provider may undertake Triage Activities as set out in the SSC Guidance for Device Security Assurance and Triage;

(b) where the assurance status is set to ‘approved' subject to conditions (as set under Section G8.36(b)) then the Triage Facility Provider will require explicit approval from the Security Sub-Committee before undertaking Triage Activities; and

(c) where the assurance status is ‘deferred’ or ‘rejected’ under Section G8.36(c) or (d), respectively, then the Triage Facility Provider is not approved to undertake Triage Activities.

Second and subsequent User Security Assessments

G12.8 Within 12 months following completion of the initial and each subsequent User Security Assessment, the Triage Facility Provider shall schedule a subsequent User Security Assessment with the User Independent Security Assurance Provider. The Security Sub-Committee shall determine the category of each such User Security Assessment to be carried out and, in doing so shall:

(a) consider any security risks identified during or since the previous User Security Assessment;

(b) take account of the volume of Devices for which Triage Activities are carried out; and

(c) reach a determination based on a proportionate assessment of the security risks as to whether the next User Security Assessment should be:

(i) a Full User Security Assessment;

(ii) a Verification User Security Assessment; or

(iii) a User Security Self-Assessment.

Definitions

G12.9 For the purpose of this Section G12:

Requestor	means an entity (such as a Party or a meter asset provider) that requests that Triage Activities are undertaken by a Triage Facility Provider.
SSC Guidance for Device Security Assurance and Triage	means the document published by the Security Sub-Committee under Section G7.19(g), which sets out guidance on the requirements and processes (including security controls and security assurance) to be followed by Triage Facility Providers undertaking Triage Activities.
Triage	means the diagnosis, upgrading or resetting of a Device.
Triage Activities	means any Triage-related activity carried out in circumstances where the SSC Guidance for Device Security Assurance and Triage requires independent assurance, including in such circumstances: a) the breach of the tamper-protection boundary; b) any unlocking of internal non-operational ports; c) any changes to the configuration of the Device Data; d) confirmation of the firmware version on the Device when Triage has been completed; and e) completion of Triage by replacing all internal non-operational port

	seals required pursuant to the CPA Security Characteristics and all tamper-protection boundary seals.
Triage Facility	means a premises where Triage Activities are undertaken.
Triage Facility Provider	means a Party which operates a Triage Facility for the purpose of carrying out Triage Activities.
Triage System Interface	means a secure virtual private network, encrypted link provided by a Manufacturer in order to connect its Triage System to a Triage Tool at a Triage Facility, which provides confidentiality and integrity of communications. The Triage System Interface: • Must use either TLS or IPsec, and • If using TLS then must include client authentication.
Triage System	means a secure IT system established for the purposes of Triage and operated by a Manufacturer, as part of its Device manufacturing capability, which the Triage Facility Provider connects to using the Triage Tool and Triage System Interface, and which is compliant with the requirements of the NCSC Commercial Product Assurance (CPA) Scheme and the associated CPA Security Characteristics.
Triage Tool	means an electronic device provided by a Manufacturer, which is used to Triage Devices in accordance with SSC Guidance for Device Security Assurance and Triage, and which is cryptographically authorised such that it can only be used for Triage Activities and cannot be given additional capabilities by an operator in a Triage Facility.

Contents

H DCC SERVICES

H1. USER ENTRY PROCESS

Eligibility Generally

H1.1 Many of the Services described in this Section H are described as being available only to Users. A Party is not entitled to receive those Services until that Party has become a User by completing the User Entry Process.

H1.2 Only persons that are Parties are eligible to complete the User Entry Process and to become Users.

User Role Eligibility

H1.3 The Services provided over the DCC User Interface are available only to Users within certain User Roles. A Party wishing to act as a User in one or more User Roles must first complete the User Entry Process for that User Role.

User IDs

H1.4 When accessing Services a User must operate in a particular User Role using the applicable User ID.

H1.5 A Party wishing to act as a User in one or more User Roles shall propose to the DCC one or more identification numbers, issued to it by the Panel, to be used by that Party when acting in each such User Role. Each such identification number must be EUI-64 Compliant, and the same identification number cannot be used for more than one User Role, save that a Party may use the same identification number when acting in any combination of some or all of the following User Roles 'Import Supplier', 'Export Supplier' and 'Gas Supplier'.

H1.6 The DCC shall accept each identification number proposed by each Party in respect of each of its User Roles (and record such numbers as identifying, and use such numbers to identify, such Party in such User Role); provided that the DCC shall only accept the proposed number if it has been issued by the Panel, and if (at the time of the Party's proposal) the Party:

(a) holds for the User Role of ‘Import Supplier’ or ‘Export Supplier’, an Electricity Supply Licence;

(b) holds for the User Role of ‘Gas Supplier’, a Gas Supply Licence;

(c) holds for the User Role of ‘Electricity Distributor’, an Electricity Distribution Licence;

(d) holds for the User Role of ‘Gas Transporter’, a Gas Transportation Licence; and

(e) is for the User Role of 'Registered Supplier Agent', identified in the Registration Data as a Meter Operator or a Meter Asset Manager for at least one MPAN or MPRN.

H1.7 A Party may from time to time replace or withdraw its User ID for each of its User Roles on notice to the DCC; provided that any such replacement shall be subject to acceptance by the DCC in accordance with Section H1.6.

User Entry Guide

H1.8 The Code Administrator shall establish and publish on the Website a guide to the User Entry Process. Such guide shall:

(a) identify the persons that a Party is required to contact to commence the steps required pursuant to the User Entry Process for each User Role; and

(b) include a recommendation that each Party undertakes a privacy impact assessment:

(i) in accordance with the Information Commissioner’s guidance concerning the same; and

(ii) where the Party is completing the User Entry Process for the User Role of Other User, having regard to any guidance issued by the Secretary of State and/or the Authority in respect of matters relating to the Processing of Personal Data that are comprised in any Data of a type referred to in Sections I1.2 to I1.4,

but there shall be no obligation under this Code to do so.

User Entry

H1.9 Where a Party wishing to become a User in a particular User Role commences the User Entry Process, it must notify the Code Administrator that it has done so (and in respect of which User Role).

User Entry Process Requirements

H1.10 The User Entry Process for each User Role requires that the Party has:

(a) received confirmation from the DCC of its acceptance of at least one User ID for the Party and that User Role in accordance with Section H1.6;

(b) successfully completed the User Entry Process Tests for that User Role in accordance with Section H14 (Testing Services);

(c) successfully demonstrated in accordance with the procedure set out in Section G8 (User Security Assurance) that the Party meets the applicable security requirements required by that Section;

(d) (in the case only of the User Role of Other User) successfully demonstrated in accordance with the procedure set out in Section I2 (Other User Privacy Audits) that the Party meets the applicable privacy requirements required by that Section; and

(e) provided the Credit Support or additional Credit Support (if any) that the DCC requires that Party to provide, to be calculated by the DCC in accordance with Section J3 (Credit Cover) as if that Party were a User for that User Role (which calculation will include the DCC's reasonable estimates of the Charges that are likely to be incurred by that Party in that User Role in the period until the first Invoice for that Party is due to be paid by that Party in that User Role).

H1.11 A Party will have successfully completed the User Entry Process for a particular User Role once the Code Administrator has received confirmation from the body responsible for each of the requirements set out in Section H1.10 that the Party has met each and every requirement set out in Section H1.10, and once the Code Administrator has confirmed the same to the Party.

H1.12 Once a Party has successfully completed the User Entry Process for a particular User Role, the Code Administrator shall confirm the same to the DCC and the Panel. A Party who has successfully completed the User Entry Processes in one User Role shall not be considered to be a User in relation to any other User Role until it has completed the User Entry Processes in relation to such other User Role.

Disputes Regarding User Entry Process

H1.13 Where a Party wishes to raise a dispute in relation to its application to become a User, and to the extent that the dispute relates to:

(a) the matters described in Section H1.10(b), then the dispute shall be determined in accordance with the applicable dispute resolution procedure set out in Section H14 (Testing Services);

(b) the matters described in Section H1.10(c), then the dispute shall be determined in accordance with the dispute resolution procedure set out in Section G8 (User Security Assurance);

(c) the matters described in Section H1.10(d), then the dispute shall be determined in accordance with the dispute resolution procedure set out in Section I2 (Other User Privacy Audits);

(d) the matters described in Section H1.10(e), then the dispute shall be determined in accordance with Section J3.15 (Disputes); or

(e) any matters other than those referred to above, then the dispute may be referred to the Panel for determination.

H1.14 Where a Party disagrees with any decision of the Panel made pursuant to Section H1.13(e), then that Party may refer the matter to the Authority for its determination, which shall be final and binding for the purposes of this Code.

Ceasing to be a User in a User Role

H1.15 Where a User wishes to cease acting as a User in a User Role, the User shall notify the Code Administrator in writing of the date from which the User wishes to cease acting as a User in that User Role.

H1.16 Where a User notifies the Code Administrator in accordance with Section H1.15, the User shall cease to be a User in the specified User Role with effect from the date specified in such notification.

H1.17 The Code Administrator shall, as soon as reasonably practicable after receipt of a notification from a User in accordance with Section H1.15, notify the Panel and the DCC of the date from which that User will cease to be a User in the specified User Role.

H1.18 Following any notification received from the Code Administrator under Section H1.17 in respect of a User and a User Role, the DCC shall cease to treat that User as a User in that User Role; provided that the DCC shall be allowed up to 24 hours from receipt of such notification to update the DCC Systems.

H2. REGISTERED SUPPLIER AGENTS

Rights and Obligations of Registered Supplier Agents

H2.1 Registered Supplier Agents are Parties to this Code in their own right, and as such have rights and obligations as Other SEC Parties or as Users acting in the User Role of Registered Supplier Agent.

Responsibility for Registered Supplier Agents

H2.2 It is acknowledged that the following Services (as described in the DCC User Interface Services Schedule) are only available to Users acting in the User Role of Registered Supplier Agent by virtue of their appointment by the Responsible Supplier as a Meter Operator or Meter Asset Manager in respect of the relevant MPAN or MPRN:

(a) Read Device Configuration;

(b) Read Event or Security Log;

(c) Read Supply Status; and

(d) Read Firmware Version.

H2.3 Without prejudice to the rights and obligations of each Registered Supplier Agent (as described in Section H2.1), the Supplier Party described in Section H2.4 shall ensure that each Registered Supplier Agent that sends Service Requests for the Services described in Section H2.2 shall only do so for the purposes of providing services to that Supplier Party in a manner consistent with that Supplier Party's Energy Supply Licence.

H2.4 The Supplier Party referred to in Section H2.3 is, in respect of a Service relating to a Smart Metering System or Device, the Responsible Supplier for that Smart Metering System or Device.

H2.5 Nothing in this Code obliges Supplier Parties to contract with Meter Operators and/or Meter Asset Managers in order to procure from the Meter Operator and/or Meter Asset Manager services that result in the need for the Meter Operator and/or Meter Asset Manager to send Service Requests.

H2.6 Each Supplier Party shall be responsible for controlling the ability of the Registered Supplier Agent to send the Service Requests referred to in Section H2.2 in circumstances where that Supplier Party would be liable under Section H2.3.

H3. DCC USER INTERFACE

Obligation to Maintain DCC User Interfaces

H3.1 The DCC shall maintain the DCC User Interface in accordance with the DCC User Interface Specification, and make it available via DCC Gateway Connections to Users to send and receive communications in accordance with the DCC User Interface Specification and the DCC User Interface Code of Connection.

H3.2 The DCC shall ensure that the DCC User Interface is available at all times (subject to Planned Maintenance undertaken in accordance with Section H8.3).

Communications to be sent via DCC User Interface

H3.3 The DCC and each User shall use the DCC User Interface for the following communications:

(a) Service Requests from a User to the DCC;

(b) Signed Pre-Commands from a User to the DCC;

(c) Acknowledgements from the DCC to a User;

(d) Pre-Commands from the DCC to a User;

(e) Service Responses from the DCC to a User;

(f) Device Alerts and DCC Alerts from the DCC to a User;

(g) Commands from the DCC to the User pursuant to the Local Command Services; or

(h) any other communications expressly required in this Code to be sent via the DCC User Interface.

H3.4 The communications required to be sent via the DCC User Interface under Section H3.3 shall only be validly sent for the purposes of this Code if sent in accordance with this Section H3, Section H4 (Processing Service Requests) and the DCC User Interface Specification.

H3.5 No Party may use the DCC User Interface for any purpose other than to meet the requirements of Section H3.3. Only the DCC and Users may use the DCC User Interface.

Eligibility for Services Over the DCC User Interface

H3.6 A User shall not send a Service Request in respect of a Smart Metering System (or a Device forming, or to form, part of a Smart Metering System) unless it is an Eligible User for that Service and Smart Metering System (save that a User may send a Service Request in circumstances where it is not an Eligible User in order to rectify errors, as further described in the Service Request Processing Document).

H3.7 Whether or not a User is an Eligible User for the following Services is determined as follows:

(a) for Enrolment Services, Core Communication Services and Local Command Services, the entitlement is described in Section H3.8; or

(b) for Elective Communication Services, the entitlement is described in the relevant Bilateral Agreement.

H3.8 Subject to Sections H3.9 to H3.10B (inclusive), the following Users are entitled to receive the following Services in respect of a Smart Metering System (or a Device forming, or to form, part of that Smart Metering System):

(a) the Import Supplier for that Smart Metering System is entitled to those Services described in the DCC User Interface Services Schedule as being available to the ‘Import Supplier’;

(b) the Export Supplier for that Smart Metering System is entitled to those Services described in the DCC User Interface Services Schedule as being available to the ‘Export Supplier’;

(c) the Gas Supplier for that Smart Metering System is entitled to those Services described in the DCC User Interface Services Schedule as being available to the ‘Gas Supplier’;

(d) the Electricity Distributor for that Smart Metering System is entitled to those Services described in the DCC User Interface Services Schedule as being available to the ‘Electricity Distributor’;

(e) the Gas Transporter for that Smart Metering System is entitled to those Services described in the DCC User Interface Services Schedule as being available to the ‘Gas Transporter’;

(f) the Registered Supplier Agent for that Smart Metering System is entitled to those Services described in the DCC User Interface Services Schedule as being available to the ‘Registered Supplier Agent’;

(g) any User acting in the User Role of Other User is entitled to those Services described in the DCC User Interface Services Schedule as being available to an ‘Other User’; and

(h) in respect of certain Services (where specified in the DCC User Interface Services Schedule) and where an electricity Smart Metering System and a gas Smart Metering System share a Communications Hub Function, the Import Supplier is entitled to those Services in respect of the gas Smart Metering System.

H3.9 Subject to Sections H3.10 and H3.10A, a User's eligibility for a Service in respect of a Smart Metering System (or a Device forming, or to form, part of that Smart Metering System) is also dependent upon the status of that Smart Metering System (or such a Device), such that:

(a) the Responsible Supplier may send Service Requests in respect of Devices that have an SMI Status of 'pending', 'whitelisted', 'installed not commissioned', 'commissioned', or 'suspended';

(b) Users that are not the Responsible Supplier may only send Service Requests in respect of Devices that have an SMI Status of 'installed not commissioned' or 'commissioned'; and

(c) Communication Services are not available in respect of a Smart Metering System until it has been Enrolled.

H3.10 Certain Services are available on the basis of Eligible User Role (rather than a User's status as an Eligible User in respect of a particular Smart Metering System or Device). In respect of these Services, references in the DCC User Interface Services Schedule to 'Electricity Import Supplier', 'Electricity Export Supplier', 'Gas Import Supplier', 'Electricity Network Operator', 'Gas Network Operator', 'Registered Supplier Agent' and 'Other Users' are to the corresponding User Roles. The Services in question are those described in the DCC User Interface Services Schedule as:

(a) 'Request WAN Matrix';

(b) 'Device Pre-notifications';

(c) 'Read Inventory';

(d) 'Communications Hub Status Update - Install Success';

(e) 'Communications Hub Status Update - Install No SM WAN';

(f) 'Communications Hub Status Update - Fault Return'; and

(g) 'Communications Hub Status Update - No Fault Return'.

H3.10A Certain Services (or certain functionality in respect of certain Services) may be identified in the DCC User Interface Services Schedule as not being available in respect of SMETS1 Devices in general or in relation to particular SMETS1 Device Models. Where this is the case, Users are not Eligible Users for the Services (or affected functionality) that are identified as being unavailable in such circumstances.

H3.10B A Party can, to the extent permitted under the Common Test Scenarios Document, complete User Entry Process Testing for a User Role (and consequently become an Eligible User for that User Role) without successfully completing testing for all the Service Requests potentially available to a User in that User Role. However, such a User will only be an Eligible User for those Service Requests in respect of which it has successfully completed testing (and not those which it has not).

Categories of Service

H3.11 Enrolment Services, Local Command Services and Core Communication Services fall into the following categories (and corresponding categories may be established in respect of Elective Communication Services under Bilateral Agreements):

(a) Services identified in the DCC User Interface Services Schedule to be available as 'on-demand' services, and which a User requests on such basis ("On-Demand Services");

(b) Services identified in the DCC User Interface Services Schedule to be available as 'future-dated' services, and which a User requests on such basis specifying the relevant time and date for execution ("Future-Dated Services"); and

(c) Services identified in the DCC User Interface Services Schedule to be available as 'scheduled' services, and which a User requests on such basis specifying the initial time and date for execution as well as the frequency at which execution is to recur ("Scheduled Services").

H3.12 The DCC shall only accept a Service Request for a Future-Dated Service or a Scheduled Service that has an execution date that is later than the time on the date at which the Service Request is received by the DCC. No User may request a Future- Dated Service that has an execution date of more than 30 days after the date on which the Service Request is sent to the DCC.

Sequenced Services

H3.13 An On-Demand Service or a Future-Dated Service may also be requested on the basis that it is only to be provided following the successful execution of a specified Service Request ("**Sequenced Services**").

Target Response Times

H3.14 The DCC shall (subject to Section H3.15) undertake the following activities within the following time periods (each such time period being, in respect of each such activity, the "**Target Response Time**" for that activity, subject to Section H3.15):

(a) Transforming Critical Service Requests into Pre-Commands and sending to the relevant User, within 3 seconds from receipt of the Service Request;

(b) sending a User a Service Response in respect of a Non-Critical Service Request for an On-Demand Service that is not a Sequenced Service, within the applicable time period set out in the DCC User Interface Services Schedule measured from receipt of the Service Request from the User;

(c) sending a User a Service Response in respect of a Critical Service Request for an On-Demand Service that is not a Sequenced Service, within the applicable time period set out in the DCC User Interface Services Schedule measured from receipt of the Signed Pre-Command from the User;

(d) sending a User a Service Response in respect of a Service Request for an On- Demand Service that is a Sequenced Service, within the applicable time period set out in the DCC User Interface Services Schedule measured from the receipt by the DCC of the Service Response for the Service Request upon which the Sequenced Service is dependent;

(e) sending a User a Service Response in respect of a Service Request for a Future- Dated Service that is not a Sequenced Service or for a Scheduled Service, within the applicable time period set out in the DCC User Interface Services Schedule measured from the time and date for execution specified in the Service Request;

(f) sending a User a Service Response in respect of a Service Request for a Future- Dated Service that is a Sequenced Service, within the applicable time period set out in the DCC User Interface Services

Schedule measured from the receipt by the DCC of the Service Response for the Service Request upon which the Sequenced Service is dependent;

(g) (except for the Alerts referred to in (h), (i) and (j) below, and except for any Alerts consolidated in accordance with the Alert Management Mechanism) sending a User an Alert, within 60 seconds measured from the Alert being communicated to (Device Alerts) or generated by (Non-Device Alerts) the Communications Hub Function;

(h) for the Services Request 'Update Device Configuration (Billing Calendar)', in addition to the above response times applicable to the Service Response confirming the configuration, periodic Alerts will be generated as a result of such configuration, for which the response time for sending the Alert to the User shall be within 24 hours from the relevant data having been communicated to the Communications Hub Function;

(i) for the Alert 'Power Outage Event (AD1)', in relation to a CSP System either predominantly based on second or third generation cellular technology or predominantly based on long-range radio technology as the SM WAN for the purposes of communicating with a particular Communications Hub, sending a User an Alert within the time as stated within the Power Outage & Restoration Alerts Delivery Management Document, measured from the time that the Alert is generated by the Communications Hub Function; and

(j) for the Alerts 'Supply Outage Restored (0x8F35)' and 'Supply Outage Restored – Outage >= 3 minutes (0x8F36)' in relation to a CSP System either predominantly based on second or third generation cellular technology or predominantly based on long-range radio technology as the SM WAN for the purposes of communicating with a particular Communications Hub, sending a User an Alert within the time as stated within the Power Outage & Restoration Alerts Delivery Management Document, measured from the time that an Alert is generated by the Electricity Smart Meter.

H3.14A For clarity, where the DCC uses a CSP System other than a CSP System predominantly based on second or third generation cellular technology or predominantly based on long-range radio technology as the SM WAN for the purposes of communicating with a Communications Hub, then Section H3.14(i) and Section H3.14(j) shall not apply and all Alerts will be subject to Section H3.14(g).

H3.14B For the Alerts which are subject to Section H3.14(i) or H3.14(j), the Target Response Times, the methodology for reviewing and determining these times, and any exclusions that shall be applied in determining whether these times have been met shall be set out in the Power Outage & Restoration Alerts Delivery Management Document. The Power Outage & Restoration Alerts Delivery Management Document shall be reviewed at least annually by the DCC in consultation with the Parties. Any changes to the Power Outage & Restoration Alerts Delivery Management Document shall be prepared and consulted upon by the DCC and approved by the Panel. Following each review of the document and its approval by the Panel, the new Target Response Times for the forthcoming year will be established and applied using the updated methodology. In preparing and consulting on any changes to the document, the DCC shall seek and pay particular attention to views given by Electricity Network Parties.

H3.15 The Target Response Times set out in Section H3.14 shall not apply to activities in respect of SMETS1 Devices, and the Target Response Times for activities in respect of SMETS1 Devices shall instead be determined in accordance with the DCC User Interface Services Schedule. For the purposes of Section H3.14 and activities in respect of SMETS2+ Devices:

(a) the concepts of 'sending' and 'receipt' are to be interpreted in accordance with the explanation of those concepts in the DCC User Interface Specification;

(b) any time during which an anomalous communication is quarantined by the DCC in accordance with Section H4 (Processing Service Requests) shall be disregarded for the purpose of measuring Response Times; and

(c) the time taken by the Communications Hub Function in communicating with the other Devices forming part of a Smart Metering System shall be disregarded.

Inherent Restrictions Linked to Technical Specifications

H3.16 The Services set out in the DCC User Interface Services Schedule are available only insofar as the minimum functionality of Devices as described in the Technical Specifications (or, to the extent required to support that minimum functionality, the GB Companion Specification or SMETS1 Supporting Requirements) allows for such Services. Any Services required in respect of additional functionality of Devices should be requested as Elective Communication Services. This Section H3.16 does not apply in respect of Services to which Non-Device Service Requests apply.

Change of Tenancy

H3.17 As soon as reasonably practicable after a Responsible Supplier for an Enrolled Smart Metering System relating to a premises becomes aware of a change of occupancy at that premises, that Responsible Supplier shall send a 'Restrict Access for Change of Tenancy' Service Request to the DCC in relation to the Smart Meter and any Gas Proxy Function forming part of that Smart Metering System (except where the out- going Energy Consumer has indicated that they wish historic information on the Smart Metering System to remain available to be viewed).

Cancellation of Future-Dated and Scheduled Services

H3.18 As soon as reasonably practicable after receipt by the DCC of a Service Response from a Smart Metering System in respect of a 'Restrict Access for Change of Tenancy' Service Request, the DCC shall cancel any and all Service Requests for Future-Dated Services or Scheduled Services in respect of any Device forming part of that Smart Metering System for which the Command has not yet been sent and which are being processed on behalf of an Other User (and shall notify the relevant User of such cancellation via the DCC User Interface).

H3.19 [Not used]

H3.20 The DCC shall cancel any and all Service Requests for Future-Dated Services or Scheduled Services for which the Command has not yet been sent and which are due to be undertaken in respect of a Device after the Decommissioning or Suspension of that Device (and shall notify the relevant User of such cancellation via the DCC User Interface).

Managing Demand for DCC User Interface Services

H3.21 During the months of January, April, July and October, by the 15th Working Day of the month, the DCC shall provide to the Panel and all Users the DCC's forecast of the number of Service Requests that all Users will (collectively) send in each of the 6 months following the end of the month in which such forecast is provided. Such forecast shall contain a breakdown of the total number of Service Requests by reference to each Service Reference Variant listed in the DCC User Interface Services Schedule; provided that for Service Reference Variant 11.1 (Update Firmware), the forecast must predict the aggregate number of Device upgrade requests that will be specified in the Service Requests (rather than the number of Service Requests). Each such forecast must specify the DCC's estimate of the number of Smart Meter installations and Enrolments which all Users will (collectively) undertake during each relevant month (recognising that such installations and Enrolments drive Service Request volumes).

H3.22 The DCC shall produce, periodically review and update, and apply a methodology (including applicable assumptions) for creating the DCC's forecasts under Section H3.21. The DCC shall share such methodology (and updates) with the Panel and Users, and the DCC shall take into account any comments on such methodology received from the Panel and Users. In producing its forecasts under Section H3.21, the DCC shall take into account any and all information provided by Users under Section H3.25.

H3.23 The DCC shall monitor and record the aggregate number of Service Requests sent by each User in total, and also the aggregate number of Service Requests sent by each User in respect of each Service Reference Variant listed in the DCC User Interface Services Schedule. In addition, for Service Reference Variant 11.1 (Update Firmware), the DCC shall monitor and record the aggregate number of Device upgrade requests specified in Service Requests.

H3.24 During the months of February, May, August and November, by no later than the 10th Working Day of the month, the DCC shall provide to the Panel and all Users a report which sets out:

(a) the aggregate number of Service Requests sent by all Users (collectively) during each of the previous 3 months (in total and broken down by reference to each Service Reference Variant listed in the DCC User Interface Services Schedule, and by number of Device upgrade requests for Service Reference Variant 11.1 (Update Firmware)), and comparing the actual numbers sent against the numbers most recently forecast for the applicable month;

(b) the DCC's assessment as to the cause of any significant deviation (taking into account any directions of the Panel concerning significance) between the DCC's forecasts and the actual numbers under paragraph (a) above, and the DCC's proposed corrective action; and

(c) the current value (calculated at the end of each of the previous three months) for every Monthly Service Metric (measured across all Users collectively) and a comparison of the current value against the relevant Monthly Service Threshold.

H3.25 Each User has the option (but no obligation) to review the (collective) forecasts and reports on actuals produced by the DCC under Sections H3.21 and H3.24. Each User has the option (but no obligation) to notify the DCC where the User disagrees with the DCC's forecast (recognising that the forecasts relate to Users collectively, and each User will only be aware of matters relating to itself), including where the User is aware of expected changes to one or more of the following (each of which will apply by reference to any threshold or other guidelines approved by the Panel from time to time):

(a) the User's daily/monthly distribution or volume of Service Requests;

(b) the User's monthly Smart Meter installation capacity;

(c) firmware releases for the User's Devices; and/or

(d) tariff updates for the User's customers.

H3.26 The Panel shall maintain and publish a list of priority Service Requests (if any) in respect of which the DCC must focus its efforts in achieving forecasting accuracy under Section H3.21. A Service Request shall only be added or removed from the list on the application of one or more Users or the DCC, and where the Panel considers the addition or removal to be reasonable in circumstances. The Panel shall publish the list from time to time on the Website, and shall give the DCC and each User advance notice of any changes to the list.

H3.27 The DCC shall, on or around each anniversary of the date on which it first started providing Services over the DCC User Interface, review (and report to the Panel on) each Monthly Service Metric and associated Monthly Service Threshold to establish whether they are still an appropriate mechanism to illustrate User behaviour that may utilise a significant element of the capacity requirements of the Services.

H3.28 The DCC shall not be considered to be in breach of this Code with regard to the obligation to achieve Target Response Times if, for the month in question:

(a) the aggregate Service Requests sent by all Users exceeds 110% of the aggregate demand most recently forecast by the DCC for that month for all Users pursuant to Section H3.21;

(b) the DCC can demonstrate to the Panel's reasonable satisfaction that the DCC did not receive comments or other information (including revisions to Anomaly Detection Thresholds) from Users which should reasonably have led the DCC to change its forecasts; and

(c) provided that the DCC shall nevertheless in such circumstances take reasonable steps to achieve the Target Response Times.

H4. PROCESSING SERVICE REQUESTS

Introduction

H4.1 The request by Users, and the provision by the DCC, of certain Services is achieved by means of the sending of communications in accordance with Section H3.3 (Communications to be Sent via the DCC User Interface) and this Section H4. The Services in question are:

(a) Enrolment Services;

(b) Local Command Services;

(c) Core Communication Services; and

(d) Elective Communication Services.

Processing Obligations

H4.2 Each User and the DCC shall each comply with the applicable obligations set out in the Service Request Processing Document concerning the secure processing of the communications required to be sent via the DCC User Interface.

DCC IDs

H4.3 The DCC shall obtain and use EUI-64 Compliant identification numbers for the purposes of its communications under this Code. Where it is expedient to do so, the DCC may use different identification numbers to identify different DCC roles.

H4.4 The DCC shall:

(a) where Section G (Security) requires it to Separate one part of the DCC Systems from another part of the DCC Systems, use different identification numbers for the purposes of its communications from each such part of the DCC Systems; and

(b) use different identification numbers for the purposes of becoming a Subscriber for different Organisation Certificates or OCA Certificates with different Remote Party Role Codes.

H5. SMART METERING INVENTORY AND ENROLMENT SERVICES

Overview of Enrolment

H5.1 Enrolment of a Smart Metering System occurs:

(a) in the case of electricity, on the Commissioning of the Electricity Smart Meter forming part of that Smart Metering System; or

(b) in the case of gas, on the Commissioning of both the Gas Smart Meter and the Gas Proxy Function forming part of that Smart Metering System.

H5.2 No Device that is to form part of a Smart Metering System (other than the Communications Hub Function) can be Commissioned before the Communications Hub Function that is to form part of that Smart Metering System has been Commissioned.

H5.3 No Device can be Commissioned:

(a) unless it is listed on the Smart Metering Inventory; and

(b) other than for Type 2 Devices, if it is listed with an SMI Status of 'decommissioned'.

Statement of Service Exemptions

H5.4 In accordance with Condition 17 of the DCC Licence (and notwithstanding any other provision of this Section H5), the DCC is not obliged to Commission Communications Hub Functions (or therefore to Enrol Smart Metering Systems) where it is exempted from the requirement to do so in accordance with a Statement of Service Exemptions.

Smart Metering Inventory

H5.5 The DCC shall establish and maintain the Smart Metering Inventory in accordance with the Inventory, Enrolment and Decommissioning Procedures.

H5.6 Each User and the DCC shall each comply with the applicable obligations set out in the Inventory, Enrolment and Decommissioning Procedures, which must include obligations concerning:

(a) the addition and removal of Devices to and from the Smart Metering Inventory; and

(b) changes to the SMI Status of the Devices recorded on the Smart Metering Inventory from time to time.

Enrolment of Smart Metering Systems

H5.7 Each User and the DCC shall each comply with the applicable obligations set out in the Inventory, Enrolment and Decommissioning Procedures Document, which must include obligations concerning:

(a) steps to be taken before a Device that is listed on the Smart Metering Inventory is installed and/or Commissioned at a premises;

(b) steps to be taken in order to Commission such a Device;

(c) steps to be taken following the Commissioning of such a Device; and

(d) steps to be taken on the removal and/or replacement of any Device forming part of a Smart Metering System.

SMETS1

H5.8 A SMETS1 Smart Metering System is eligible to be Enrolled when the combination of SMETS1 Devices of which it is comprised form all or part of a SMETS1 Installation for which all the Devices are of Device Models which either:

(a) comprise a combination of Device Models listed on the SMETS1 Eligible Product Combinations; or

(b) could as a result of the application of an existing firmware upgrade or upgrades become a combination of Device Models listed on the SMETS1 Eligible Product Combinations.

H5.9 The DCC shall only be required to Enrol SMETS1 Smart Metering Systems, or process Service Requests in respect of SMETS1 Smart Metering Systems, that comprise a combination of Device Models that is listed on the SMETS1 Eligible Product Combinations or that contain a Non-EPCL Device Model.

H5.10 The Inventory, Enrolment and Decommissioning Procedures Document may also set out circumstances in which the Panel may direct the DCC not to Commission a SMETS1 Device (or purported SMETS1 Device).

H6. DECOMMISSIONING AND SUSPENSION OF DEVICES

Decommissioning

H6.1 Where a Device other than a Type 2 Device is no longer to form part of a Smart Metering System, then that Device should be Decommissioned. A Device may be Decommissioned because it has been uninstalled and/or is no longer operating (whether or not it has been replaced, and including where the Device has been lost, stolen or destroyed).

H6.2 Only the Responsible Supplier(s) for a Communications Hub Function, Smart Meter, Gas Proxy Function, Standalone Auxiliary Proportional Controller or Type 1 Device may Decommission such a Device; provided that only the Lead Supplier may Decommission a SMETS1 CHF.

H6.3 Where a Responsible Supplier (or, in the case of a SMETS1 CHF, the Lead Supplier) becomes aware that a Device has been uninstalled and/or is no longer operating, that User shall send a Service Request requesting that it is Decommissioned.

H6.4 On successful processing of a Service Request from a User in accordance with Section H6.3, the DCC shall:

(a) set the SMI Status of the Device to ‘decommissioned’;

(b) where relevant, amend the Smart Metering Inventory so that the Device is no longer Associated with any other Devices; and

(c) where the Device in question is a Communications Hub Function, notify any and all Responsible Suppliers (other than the Responsible Supplier that procured such Decommissioning) for that Communications Hub Function of such Decommissioning.

H6.5 Where the DCC receives a Service Request from a User that does not satisfy the requirements of Section H6.2, the DCC shall reject the Service Request.

H6.6 On the Decommissioning of a Communications Hub Function, the other Devices forming part of a Smart Metering System should also be Decommissioned; provided that the Devices forming part of a Smart Metering System (other than the Gas Proxy Function) may remain Commissioned notwithstanding the Decommissioning of the Communications Hub Function if a replacement Communications Hub Function is Commissioned within a reasonable period.

H6.7 [Not used]

H6.8 [Not used]

H6.9 [Not used]

Suspension

H6.10 Where a Device’s Device Model is removed from the Central Products List, that Device shall be Suspended and the DCC shall set the SMI Status of the Device to ‘suspended’.

H6.11 Where a Communications Hub Device Model is removed from the Central Products List, both the Communications Hub Function and the Gas Proxy Function shall be deemed to be Suspended (and Section H6.10 shall apply accordingly).

Ancillary Obligations

H6.12 Each User and the DCC shall each comply with the obligations set out in the Inventory, Enrolment and Decommissioning Procedures concerning Decommissioning and Suspension of Devices (and the Smart Metering Systems of which such Devices form part), including (where applicable) notifying other Users of such Decommissioning and Suspension.

H7. ELECTIVE COMMUNICATION SERVICES

Eligible Smart Metering Systems

H7.1 Elective Communication Services can only be provided in respect of Smart Metering Systems that have been Enrolled.

Entitlement to Elective Communication Services

H7.2 Only a User is entitled to receive Elective Communication Services. A Party that is not a User is not entitled to receive Elective Communication Services.

H7.3 A User shall not be entitled to request or receive (and the DCC shall not provide to such User) any Elective Communication Services that would constitute a Restricted Communication Service.

Preliminary Assessment of Elective Communication Services

H7.4 Notwithstanding Section H7.1 and H7.2, any Party may request an initial evaluation of the technical feasibility and likely Charges for a proposed Elective Communication Service (a "**Preliminary Assessment**").

H7.5 Requests for a Preliminary Assessment shall be made in such format as the DCC may specify from time to time, and shall be submitted to the DCC.

H7.6 The DCC shall respond to requests for a Preliminary Assessment in accordance with the time period prescribed by Condition 17 of the DCC Licence, and shall either (in accordance with Condition 17 of the DCC Licence):

(a) provide an initial evaluation of the technical feasibility and the likely Charges for a proposed Elective Communication Service; or

(b) give notice that a further and more detailed evaluation of the request is required.

Detailed Evaluation of Elective Communication Services

H7.7 Any Party that has requested a Preliminary Assessment and obtained a response as described in Section H7.6(b) may request a more detailed evaluation of the technical feasibility and likely Charges for a proposed Elective Communication Service (a "**Detailed Evaluation**").

H7.8 Requests for a Detailed Evaluation shall be made in such format as the DCC may specify from time to time, and shall be submitted to the DCC. Following receipt of any such request (or purported request), the DCC shall:

(a) where the request is incomplete or the DCC reasonably requires further information in order to assess the request, notify the Party that this is the case and provide reasonable assistance to the Party in re-submitting its request;

(b) once the DCC has received all the information it reasonably requires in order to assess the request, confirm the applicable Charges payable in respect of the Detailed Evaluation; and

(c) once the Party has agreed to pay the applicable Charges, provide the Detailed Evaluation to the requesting Party (in accordance with the time period prescribed by Condition 17 of the DCC Licence).

Request for an Offer for an Elective Communication Service

H7.9 Any Party that has requested a Preliminary Assessment in respect of a proposed Elective Communication Service, and obtained a response as described in Section H7.6(a), may request a formal offer for that proposed Elective Communication Service.

H7.10 Any Party that has requested and obtained a Detailed Evaluation in respect of a proposed Elective Communication Service may request a formal offer for that proposed Elective Communication Service.

H7.11 Following a request pursuant to Section H7.9 or H7.10, the DCC shall (in accordance with the time period prescribed by Condition 17 of the DCC Licence):

(a) make an offer to provide the Elective Communication Service in question; or

(b) notify the Party that the DCC is not willing to make such an offer (provided that the DCC may only do so where the DCC is not obliged to make such an offer in accordance with Condition 17 of the DCC Licence).

Formal Offer

H7.12 An offer to provide the Elective Communication Service made by the DCC pursuant to this Section H7 shall:

(a) include details of the Charges that would apply to the Elective Communication Service, as determined in accordance with the Charging Methodology;

(b) where the proposed Charges have been calculated (in accordance with the Charging Methodology) on the assumption that one or more other Parties accept offers made pursuant to this Section H7, provide for two alternative sets of Charges, one of which is contingent on acceptance of all the other such offers and one of which is not; and

(c) include an offer by the DCC to enter into a Bilateral Agreement with the Party requesting the Elective Communication Service.

H7.13 Each Bilateral Agreement must:

(a) be based on the Specimen Bilateral Agreement, subject only to such variations from such specimen form as are reasonable in the circumstances;

(b) not contradict or seek to override any or all of this Section H or Sections G (Security), I (Data Privacy), J (Charges), L (Smart Metering Key Infrastructure) or M (General);

(c) where reasonably necessary in accordance with the Charging Methodology, provide for Charges that include or comprise a standing charge that is payable by the recipient of the Elective Communication Service regardless of whether or not the Elective Communication Service is requested or provided;

(d) where reasonably necessary in accordance with the Charging Methodology, require the recipient of the Elective Communication Service to pay compensation to DCC in the event of the early termination of the Bilateral Agreement (except in the case of termination as envisaged by Section H7.13(e));

(e) allow the recipient of the Elective Communication Services to terminate the Bilateral Agreement without paying compensation to the extent that such compensation is intended to recover investments made for the purposes of providing the Elective Communication Service where (and to the extent that) the DCC subsequently offers a Service listed in the DCC User Interface Services Schedule that relies upon such investments (and each Bilateral Agreement must provide for disputes regarding this provision to be subject to an initial Panel determination, but to ultimately be determined by arbitration); and

(f) where reasonably necessary, require the recipient of the Elective Communication Services to provide credit support in respect of its obligation to pay the compensation referred to in Section H7.13(d).

H7.14 The parties to each Bilateral Agreement shall ensure that the Bilateral Agreement describes the Elective Communication Services in a manner consistent with the description of the Core Communication Services in this Code, including so as to identify (to the extent appropriate) equivalents of the following concepts: Service Requests; Non-Device Service Requests; Pre-Commands; Signed Pre-Commands; Commands; Services Responses; Alerts; and Target Response Times. To the extent that an Elective Communication Service comprises equivalents of such concepts, references to such concepts in this Code shall be construed as including the equivalent concepts under each Bilateral Agreement (and the DCC and the relevant User under the Bilateral Agreement shall comply with Sections H3 (DCC User Interface) and H4 (Processing Service Requests) in respect of the same). For the purposes of each Elective Communication Service (unless the Panel otherwise determined on a User's application):

(a) the applicable Service Request shall be deemed to be a Critical Service Request, unless it results only in the sending of a Command to a Device that would arise were a Non-Critical Service Request listed in the DCC User Interface Service Schedule to be requested; and

(b) other than in the case of SMETS1 Service Requests, the applicable Service Request (and any associated Pre-Command) shall be deemed to contain Data that requires Encryption, unless it contains only Data described in the GB Companion Specification as capable of being sent without Encryption.

H7.15 Elective Communication Services shall be provided in accordance with this Code and the applicable Bilateral Agreement. In the event of any inconsistency between this Code and a Bilateral Agreement, the provisions of this Code shall prevail.

H7.16 The DCC shall not agree to any variations to a Bilateral Agreement that would cause that agreement to become inconsistent with the requirements of this Section H7.

Disputes Regarding Offers for Elective Communication Services

H7.17 Where the requirements of Condition 20 of the DCC Licence are met, a Party that has requested an offer for a proposed Elective Communication Service may refer a dispute regarding such request to the Authority for determination under and in accordance with that Condition.

Publication of Details of Elective Communication Services

H7.18 Once the DCC has commenced provision of an Elective Communication Service pursuant to a Bilateral Agreement, the DCC shall notify the Code Administrator of the date on which the provision of such service commenced (but shall not provide any details regarding such agreement to the Code Administrator).

H7.19 The DCC shall, on or around the date falling six months after it commenced provision of an Elective Communication Service pursuant to a Bilateral Agreement, provide to the Code Administrator the following details:

(a) a brief description of the Elective Communication Service;

(b) the frequency with which, and (where stated) the period during which, the Elective Communication Service is to be provided; and

(c) the Target Response Time within which the Elective Communication Service is to be provided.

H7.20 The Code Administrator shall arrange for the publication on the Website of the details provided to it pursuant to Section H7.19. The Code Administrator shall monitor and report to the Panel on whether the DCC has provided details pursuant to Section H7.18 in respect of Elective Communication Services of which the Code Administrator is notified under Section H7.18.

H7.21 Without prejudice to the DCC's obligations under Section H7.19, the existence and contents of each Bilateral Agreement shall constitute Confidential Information which the DCC is obliged to keep confidential in accordance with Section M4 (Confidentiality).

H8. SERVICE MANAGEMENT, SELF-SERVICE INTERFACE AND SERVICE DESK

General

H8.1 The DCC shall provide the Services in a manner that is consistent with:

(a) the Service Management Standards; or

(b) any other methodology for service management identified by the DCC as being more cost efficient than the Service Management Standards, and which has been approved by the Panel for such purpose.

Maintenance of the DCC Systems

H8.2 The DCC shall (insofar as is reasonably practicable) undertake Maintenance of the DCC Systems in such a way as to avoid any disruption to the provision of the Services (or any part of them).

H8.3 Without prejudice to the generality of Section H8.2, the DCC shall (unless the Panel agrees otherwise and subject to any contrary provisions in the SEC Subsidiary Documents applying in relation to the SMETS1 SM WAN and/or the Systems of the SMETS1 Service Providers):

(a) categorise Planned Maintenance changes into Low Impact Planned Maintenance or High Impact Planned Maintenance;

(b) undertake Planned Maintenance of the DCC Systems only between 20.00 hours and 08.00 hours;

(c) limit High Impact Planned Maintenance of the DCC Systems generally to two windows which have a maximum total duration of six hours per month; and

(d) limit Low Impact Planned Maintenance of the DCC Systems generally (including of the Self-Service Interface) to six windows per month of no more than six hours each.

H8.4 At least 20 Working Days prior to the start of each month, the DCC shall make available to Parties, to Registration Data Providers and to the Panel a schedule of the Planned Maintenance for that month (subject to any contrary provisions in the SEC Subsidiary Documents applying in relation to the SMETS1 SM WAN and/or the Systems of the SMETS1 Service Providers). Such schedule shall set out (as a minimum) the following:

(a) the proposed Maintenance activity (in reasonable detail);

(b) the parts of the Services that will be disrupted (or in respect of which there is a Material Risk of disruption) during each such Maintenance activity;

(c) the time and duration of each such Maintenance activity; and

(d) any associated risk that may subsequently affect the return of normal Services.

H8.4A Where an additional Planned Maintenance is required beyond that set out pursuant to Section H8.4, the DCC shall revise and reissue the schedule of Planned Maintenance:

(a) at least 10 Working Days in advance of any additional Low Impact Planned Maintenance; and

(b) at least 20 Working Days in advance of any additional High Impact Planned Maintenance.

H8.5 The Panel may (whether or not at the request of a Party and subject to any contrary provisions in the SEC Subsidiary Documents applying in relation to the SMETS1 SM WAN and/or the Systems of the SMETS1 Service Providers) request that the DCC reschedules any Planned Maintenance set out in a monthly schedule provided pursuant to Section H8.4. In making any such request, the Panel shall provide the reasons for such request to the DCC in support of the request. The DCC will take all reasonable steps to accommodate any such request.

H8.6 As soon as reasonably practicable after the DCC becomes aware of any Unplanned Maintenance, the DCC shall notify the Panel, Parties and (insofar as they are likely to be affected by such Unplanned Maintenance) Registration Data Providers of such Unplanned Maintenance (and shall provide information equivalent to that provided in respect of Planned Maintenance pursuant to Section H8.4).

H8.7 During the period of any Planned Maintenance or Unplanned Maintenance, the DCC shall provide Parties and (insofar as they are likely to be affected by such maintenance) Registration Data Providers with details of its duration and the expected disruption to Services to the extent they differ from the information previously provided.

DCC Internal System Changes

H8.8 Where the DCC is proposing to make a change to DCC Internal Systems, the DCC shall:

(a) undertake an assessment of the likely impact on:

(i) Parties in respect of any potential disruption to Services; and/or

(ii) RDPs in relation to the receipt of data pursuant to Section E (Registration Data),

that may arise as a consequence of the Maintenance required to implement the contemplated change;

(b) where such assessment identifies that there is a Material Risk of disruption to Parties and/or RDPs, consult with Parties and/or RDPs (as applicable) and with the Panel regarding such risk;

(c) provide the Parties and RDPs the opportunity to be involved in any testing of the change to the DCC Internal Systems prior to its implementation; and

(d) undertake an assessment of the likely impact of the contemplated change upon the security of the DCC Total System, Smart Metering Systems, and the Systems of Parties and/or RDPs.

Release Management

H8.9 The DCC shall ensure that it plans, schedules and controls the building, testing and deployment of releases of IT updates, procedures and processes in respect of the DCC Internal Systems and/or the Parse and Correlate Software in accordance with a policy for Release Management (the "**DCC Release Management Policy**").

H8.10 The DCC shall ensure that the DCC Release Management Policy:

(a) defines the scope of the matters that are to be subject to the policy in a manner consistent with the Service Management Standards;

(b) includes a mechanism for setting priorities for different types of such matters;

(c) defines periods of change-freeze where no such matters may be implemented; and

(d) defines periods of notice to be given to Parties and RDPs prior to the implementation of such matters.

H8.11 The DCC shall make the DCC Release Management Policy available to Parties, RDPs and the Panel. The DCC shall consult with Parties, RDPs and the Panel before making any changes to the DCC Release Management Policy.

H8.12 The DCC's obligation under Section H8.11 is in addition to its obligations in respect of Planned Maintenance and changes to DCC Internal Systems to the extent that the activity in question involves Planned Maintenance or changes to DCC Internal Systems.

Self-Service Interface and Service Desk: General

H8.13 Each User shall take reasonable steps to access the information it needs, and to seek to resolve any queries it may have, via the Self-Service Interface in the first instance. A User shall only contact the Service Desk where it cannot reasonably obtain the information it needs, or resolve its query, via the Self-Service Interface.

H8.14 A Party that is not a User will be unable to access the Self-Service Interface, but may contact the Service Desk.

Self-Service Interface

H8.15 The DCC shall maintain and keep up-to-date an interface (the **Self-Service Interface**) which:

(a) complies with the specification required by the Self-Service Interface Access Control Specification and the SSI Baseline Requirements Document;

(b) is made available to Users in accordance with the Self-Service Interface Code of Connection via DCC Gateway Connections; and

(c) allows each User to access the information described in Section H8.16 as being accessible to that User (and also allows other Users to access that information to the extent permitted by the first User in accordance with the Self-Service Interface Access Control Specification).

H8.15A Any changes to the Self-Service Interface shall be processed by the DCC in accordance with the **"SSI Change Governance Process"**. Any changes to the SSI Change Governance Process shall be prepared and consulted upon by the DCC and approved by the Panel.

H8.16 The Self-Service Interface must (as a minimum) allow the following categories of User to access the following:

(a) the Smart Metering Inventory, which shall be available to all Users and capable of being searched by reference to the following (provided that there is no requirement for the DCC to provide information held on the inventory in respect of Type 2 Devices other than IHDs):

(i) the Device ID, in which case the User should be able to extract all information held in the inventory in relation to (I) that Device, (II) any other Device Associated with the first Device, (III) any Device Associated with any other such Device; and (IV) any Device with which any of the Devices in (I), (II) or (III) is Associated;

(ii) the MPAN or MPRN, in which case the User should be able to extract all information held in the inventory in relation to the Smart Meter to which that MPAN or MPRN relates, or in relation to any Device Associated with that Smart Meter or with which it is Associated;

(iii) post code and premises number or name, in which case the User should be able to extract all information held in the inventory in relation to the Smart Meters for the MPAN(s) and/or MPRN linked to that postcode and premises number or name, or in relation to any Device Associated with those Smart Meters or with which they are Associated; and

(iv) the UPRN (where this has been provided as part of the Registration Data), in which case the User should be able to extract all information held in the inventory in relation to the Smart Meters for the MPAN(s) and/or MPRN linked by that UPRN, or in relation to any Device Associated with those Smart Meters or with which they are Associated;

(b) a record of the Service Requests, Signed Pre-Commands, Acknowledgements, Pre-Commands, Service Responses and Alerts sent in respect of each Smart Metering System (during a period of no less than three months prior to any date on which that record is accessed), which shall be available only to the Responsible Supplier for that Smart Metering System and to the Gas Transporter or Electricity Distributor (as applicable) for that Smart Metering System;

(c) a record, which (subject to the restriction in Section I1.4 (User Obligations)) shall be available to all Users:

(i) of all 'Read Profile Data' and 'Retrieve Daily Consumption Log' Service Requests in relation to each Smart Meter (or Device Associated with it) that were sent by any User during a period of no less than three months prior to any date on which that record is accessed; and

(ii) including, in relation to each such Service Request, a record of the type of the Service Request, whether it was successfully processed, the time and date that it was sent to the DCC, and the identity of the User which sent it;

(d) the Incident Management Log, for which the ability of Users to view and/or amend data shall be as described in Section H9.4 (Incident Management Log);

(e) the CH Order Management System, which shall be available to all Users;

(f) any and all information in respect of the SMETS1 SM WAN as the DCC is required to make available under the Self-Service Interface Access Control Specification and the SSI Baseline Requirements Document, which shall be made available to all Users; and the following information in respect of the SMETS2+ SM WAN, which shall be available to all Users (and which shall be capable of interrogation by post code and postal outcode):

(i) whether a Communications Hub Function installed in a premises at any given location:
(A) is expected to be able to connect to the SM WAN;
(B) is expected to be able to connect to the SM WAN from a particular date, in which case the date shall be specified; or
(C) cannot be confirmed as being able to connect to the SM WAN;

(ii) any known issues giving rise to poor connectivity at any given location (and any information regarding their likely resolution); and

(iii) any requirement to use a particular WAN Variant (and, where applicable, in combination with any particular Communications Hub Auxiliary Equipment) for any given location in order that the Communications Hub will be able to establish a connection to the SM WAN;

(g) additional information made available by the DCC to assist with the use of the Services and diagnosis of problems, such as service status (including information in respect of Planned Maintenance and Unplanned Maintenance) and frequently asked questions (and the responses to such questions), which shall be available to all Users; and

(h) anything else expressly required by a provision of this Code.

H8.17 Without prejudice to the requirements of Sections H8.16(b) and (c), to the extent that the Self-Service Interface does not allow a User to access a record of the information referred to in those Sections in respect of the preceding 7 years, then:

(a) subject (in the case of the information referred to in Section H8.16 (c)) to the restriction in Section I1.4 (User Obligations), that User shall be entitled to request such information from the DCC; and

(b) the DCC shall provide such information to that User as soon as reasonably practicable following such request.

H8.18 The DCC shall ensure that the Self-Service Interface is available at all times (subject to Planned Maintenance undertaken in accordance with Section H8.3).

Service Desk

H8.19 The DCC shall ensure that a team of its representatives (the **Service Desk**) is available to be contacted as follows:

(a) the Service Desk shall be contactable via the following means (to be used by Parties and Registration Data Providers, to the extent available to them, in the following order of preference, save as otherwise provided for in the Incident Management Policy):

(i) the Self-Service Interface;

(ii) a dedicated email address published on the DCC Website; and

(iii) a dedicated telephone number published on the DCC Website;

(b) the Service Desk can be used by Parties to seek resolution of queries relating to the Services (provided that Users shall seek resolution via the Self-Service Interface in the first instance); and

(c) the Service Desk can be used by Incident Parties that are not Users to raise Incidents (or by Users, where the Incident Management Log is not available via the Self-Service Interface, to raise or provide information in respect of Incidents), which the DCC shall then reflect in the Incident Management Log.

H8.20 The DCC shall ensure that the Service Desk is available at all times, and shall provide alternative arrangements (a different telephone number and email address) where the usual Service Desk in not available. Where a different telephone number and email address is to be used, the DCC shall publish details of the alternative number and address at least 20 Working Days in advance.

H9. INCIDENT MANAGEMENT

Incident Management Policy

H9.1 The Incident Management Policy must (as a minimum) make provision for the following matters:

(a) raising an Incident by recording it in the Incident Management Log;

(b) categorisation of Incidents into 5 categories of severity ("**Incident Category 1, 2, 3, 4 and 5**" respectively, such that Incident Category 1 is the most severe and Incident Category 5 the least);

(c) prioritisation of Incidents, and (in those cases where the DCC is responsible for resolving an Incident) the time period within which an Incident in each Incident Category should be resolved (the "**Target Resolution Time**");

(d) prioritising and timescale for closure of Problems;

(e) allocation of responsibility for Incidents and Problems in accordance with Section H9.2;

(f) identification of other interested persons who are to be kept informed regarding Incidents;

(g) courses of action to be undertaken in seeking to resolve Incidents and close Problems, including the need to update the Incident Management Log to record activity carried out (or planned to be carried out);

(h) rules for the escalation of Incidents;

(i) rules for the declaration of a Major Incident, and for the appointment of managers to coordinate resolution of Major Incidents;

(j) rules for the closure of a resolved Incident;

(k) rules for opening and closing Problem records by the DCC;

(l) rules for reopening closed Incidents; and

(m) describe the roles and responsibilities of the following persons in respect of different types of Incident: Users, Eligible Subscribers, DCC Gateway Parties and Registration Data Providers (such persons being the "Incident Parties").

Incident and Problem Management Responsibility

H9.2 The Incident Management Policy must allocate responsibility for resolution of Incidents and closure of Problems in accordance with the following principles:

(a) where an Incident Party becomes aware of an Incident that is not yet logged on the Incident Management Log (or, if logged, is incorrectly logged as closed), and:

(i) where such Incident is reasonably capable of being resolved via the Self- Service Interface or via a Service Request which that Incident Party has the right to send, that Incident Party shall exercise such rights with a view to resolving the Incident;

(ii) where the CH Support Materials are relevant to the Incident and require the Incident Party to take any steps prior to raising an Incident, that Incident Party shall take such steps with a view to resolving the Incident; or

(iii) where the Incident Party is a Supplier Party and it is already at the premises when it first becomes aware of the Incident, and to the extent the Incident is either: (A) caused by a SMETS1 CH for which the Incident Party is the Lead Supplier; or (B) caused by a SMETS2+ Communications Hub and not capable of being resolved via communications over the SM WAN, then (in either case) that Incident Party shall be responsible for resolving that Incident;

(b) subject to Section H9.2(a), the DCC shall be responsible for resolving Incidents and closing Problems to the extent they are caused by:

(i) the DCC Systems;

(ii) the Parse and Correlate Software; or

(iii) a SMETS2+ Communications Hub, and are capable of being resolved via communications over the SM WAN;

(c) subject to Section H9.2(a), the Lead Supplier for a Communications Hub shall be responsible for resolving Incidents and closing Problems to the extent they are caused by that Communications Hub where either: (A) it is a SMETS1 CH; or (B) the Incident or Problem is not capable of being resolved or closed via communications over the SM WAN;

(d) subject to Section H9.2(a), the Responsible Supplier for a Smart Metering System shall be responsible for resolving Incidents and closing Problems to the extent caused by Devices (other than the Communications Hub) forming part of that Smart Metering System;

(e) in the case of Incidents arising in respect of the exchange of Data under Section E (Registration Data):

(i) the relevant Registration Data Provider shall be responsible for resolving those Incidents arising on its side of the Registration Data Interface; and

(ii) the DCC shall be responsible for resolving all other such Incidents; and

(f) in the case of Incidents other than those referred to elsewhere in this Section H9.2, the Incident Party assigned responsibility in accordance with the Incident Management Policy shall be responsible for resolving the Incident.

Incident Management Log

H9.3 The DCC shall maintain and keep up-to-date an electronic log (the **Incident Management Log**) that records the following in respect of each Incident:

(a) a unique reference number (to be allocated to each Incident that is identified by, or reported to, the DCC);

(b) the date and time that the Incident was identified by, or reported to, the DCC;

(c) the nature of the Incident and the location at which it occurred;

(d) whether the Incident was identified by the DCC, or otherwise the person that reported the Incident to the DCC;

(e) the categorisation of the Incident in accordance with the Incident Management Policy;

(f) the person to whom the Incident has been allocated for resolution;

(g) the course of action to be taken, or taken, to resolve the Incident;

(h) the DCC's Good Industry Practice assessment of which Incident Parties and/or Services are affected by the Incident;

(i) details of any communications with Incident Parties in respect of the Incident;

(j) comments regarding any mitigating circumstances regarding the Incident;

(k) the potential impact of the Incident on the DCC's ability to meet the Target Service Levels;

(l) the current status of the Incident, and (once applicable) the date and time that the Incident was closed; and

(m) a reference to any related Problem logged.

H9.4 The following shall apply in respect of the Incident Management Log:

(a) (subject to paragraphs (c) and (d) below) the DCC shall provide Users with the ability to view and amend the Incident Management Log via the Self Service Interface;

(b) (subject to paragraphs (c) and (d) below) the DCC shall provide Incident Parties that are not Users with the ability to obtain information from, and report information which the DCC shall then add to, the Incident Management Log via the Service Desk;

(c) only the following Incident Parties shall be entitled to view or obtain information from the Incident Management Log in respect of an Incident:

(i) the Incident Party that raised the Incident;

(ii) the Incident Party that is assigned responsibility for resolving the Incident; and

(iii) (subject to any further rules in the Incident Management Policy) the following persons:

(A) the Lead Supplier for each Communications Hub that is affected by the Incident;

(B) the Responsible Supplier for each Smart Metering System that is affected by the Incident;

(C) the Electricity Distributor or Gas Transporter (as applicable) for each Smart Metering System that is affected by the Incident;

(D) the DCC Gateway Party for, and any Party notified to the DCC in accordance with Section H15.17 (Use of a DCC Gateway Connection) as entitled to use, a DCC Gateway Connection shall be able to view matters relating to any Incident affecting that DCC Gateway Connection;

(E) the Registration Data Providers entitled to use a DCC Gateway Connection as provided for in Section E3 (DCC Gateway Connections for Registration Data Providers) shall be able to view matters relating to any Incident affecting that DCC Gateway Connection; and

(F) any other Incident Party that is reasonably likely to be affected by the Incident;

(d) only the following Incident Parties shall be entitled to amend and report information to be added to the Incident Management Log:

(i) the Incident Party that raised the Incident;

(ii) the Incident Party that is assigned responsibility for resolving the Incident; and

(iii) (subject to any further rules in the Incident Management Policy) the following persons:

(G) the Lead Supplier for each Communications Hub that is affected by the Incident (but such amending and reporting shall be limited to matters relating to the Communications Hub Function); and

(H) the Responsible Supplier(s) for each Smart Metering System that is affected by the Incident (but such amending and reporting shall exclude matters relating to the Communications Hub Function); and

(e) to the extent that an Incident Party does not have the necessary rights in accordance with paragraph (d) above to amend the Incident Management Log, an Incident Party shall report the matter to the DCC, which shall then amend the Incident Management Log to reflect such matters.

Access to data regarding Problems

H9.5 Where an Incident refers to a Problem, the DCC or any Incident Party may request that the person assigned responsibility for the Problem supplies to the DCC or Incident Party making the request reasonable information regarding the Problem, provided that information in respect of any other Incident shall only be supplied to an Incident Party where that Incident Party would be allowed access to that information in accordance with Section H9.4.

Addition of Incidents to the Incident Management Log

H9.6 Where an Incident Party becomes aware of an Incident that is not yet logged on the Incident Management Log (or, if logged, is incorrectly logged as closed):

(a) (where the Incident Party is a User) to the extent such Incident is reasonably capable of being resolved via the Self-Service Interface or via a Service Request which that User has the right to send, then the User shall exercise such rights with a view to resolving the Incident;

(b) where paragraph (a) above does not apply (or to the extent the Incident is not resolved despite compliance with paragraph (a) above), then the Incident Party shall add the Incident to the Incident Management Log (or, if incorrectly logged as closed, reopen the Incident) via the Self-Service Interface (or, in the case of non-Users, the Service Desk).

H9.7 Where the DCC becomes aware of an Incident that is not yet logged on the Incident Management Log (or, if logged, is incorrectly logged as closed), then the DCC shall add the Incident to the Incident Management Log (or, if incorrectly logged as closed, reopen the Incident).

Resolving Incidents and Closing Problems

H9.8 Where an Incident has been added to the Incident Management Log (or reopened) pursuant to Section H9.6 or H9.7, then (until such time as that Incident is closed) the DCC and each relevant Incident Party shall each take all the steps allocated to them under and in accordance with the Incident Management Policy in respect of an Incident of the relevant type, so as to:

(a) in the case of Incidents for which an Incident Party is responsible, resolve the Incident as soon as reasonably practicable; or

(b) in the case of Incidents for which the DCC is responsible, resolve the Incident in accordance with the applicable Target Resolution Time.

H9.9 Where a Problem has been assigned to the DCC or an Incident Party, then (until such time as that Problem is closed) the DCC and each relevant Incident Party shall each take all the steps allocated to it under and in accordance with the Incident Management Policy so as to close the Problem in accordance with priority for resolution and closure set out in the Incident Management Policy.

Major Incident Notification and Reports

H9.10 Where an Incident Party is identified as responsible for resolution of an Incident, and where that Incident Party considers (or should reasonably have considered) that the Incident constitutes a Major Incident, then such Incident Party shall notify the DCC of such fact (in accordance with the Incident Management Policy).

H9.11 Where the DCC becomes aware of a Major Incident, the DCC shall notify all Incident Parties that are likely to be affected by such Major Incident (in accordance with the Incident Management Policy).

H9.12 In the event of a Major Incident:

(a) where the DCC is responsible for resolving that Incident, each Incident Party shall provide the DCC with all reasonable assistance as the DCC may request; and

(b) where an Incident Party is responsible for resolving that Incident, the DCC and all other Incident Parties shall provide all reasonable assistance to the Incident Party responsible for resolving that Incident as such Incident Party may request,

(in each case) in relation to the resolution of that Incident, including as set out in the Incident Management Policy.

H9.13 Within two Working Days following resolution of a Major Incident, the DCC or the Incident Party responsible for resolving that Major Incident shall (subject to any contrary provisions in the SEC Subsidiary Documents applying in relation to the SMETS1 SM WAN and/or the Systems of the SMETS1 Service Providers) provide a summary report to the Panel in respect of that Major Incident. Such summary report must include (as a minimum):

(a) the nature, cause and impact (and likely future impact) of the Major Incident (including, where the DCC is responsible for resolving the Major Incident, details of the impact the Major Incident had on provision of the Services and over what period, and details of any Data that may have been lost); and

(b) the action taken in the resolution of the Major Incident.

H9.14 Within 20 Working Days following resolution of a Major Incident, the DCC or Incident Party responsible for resolving that Major Incident shall (subject to any contrary provisions in the SEC Subsidiary Documents applying in relation to the SMETS1 SM WAN and/or the Systems of the SMETS1 Service Providers) conduct a review regarding that Major Incident and its resolution, and shall report to the Panel and the Authority (and, on request, the Secretary of State) on the outcome of such review. Such report must include (as a minimum):

(a) a copy of the summary report produced in respect of the Major Incident pursuant to Section H9.13;

(b) (where the DCC is responsible for resolving the Major Incident) any Services which were not restored within the Target Resolution Time for the Major Incident;

(c) (where the DCC is responsible for resolving the Major Incident) where any Services were not restored within the Target Resolution Time, the reason why this was the case and the steps the DCC is taking to prevent the re-occurrence of such an event;

(d) a review of the response to the Major Incident and its effectiveness;

(e) any failures by Incident Parties to comply with their obligations under Energy Licences and/or this Code that caused or contributed to the Major Incident or its consequences;

(f) (where the DCC is responsible for resolving the Major Incident) whether there is likely to be a reduction (and, to the extent reasonably capable of being determined at that time, the amount of the anticipated reduction) in the DCC's External Costs (as defined in the DCC Licence) arising as a consequence of the DCC Service Providers failing to achieve a restoration of any Services within the Target Resolution Time; and

(g) any Modifications that could be made to this Code to mitigate against future Incidents and/or their consequences.

H9.15 The Panel shall make each report produced by the DCC pursuant to Section H9.14 available to the other Parties, subject to any redactions it considers necessary to avoid a risk of Compromise to the DCC Total System, User Systems, RDP Systems and/or Devices.

Disputes

H9.16 Where Disputes arise between the Incident Parties regarding whether or not the DCC and/or an Incident Party has complied with its obligations under this Section H9, then such Dispute shall be subject to determination by the Panel (which determination shall be final and binding).

H10. BUSINESS CONTINUITY

Emergency Suspension of Services

H10.1 Section H10.2 applies in respect of any Party or RDP which has an established DCC Gateway Connection where, by virtue of the action or failure to act of that Party or RDP, or of any event occurring on or in relation to the Systems of that Party or RDP:

(a) the DCC Systems are being Compromised to a significant extent; or

(b) the DCC has reason to believe that there is an immediate threat of the DCC Systems being Compromised to a significant extent.

H10.2 Where this Section H10.2 applies, the DCC may, to the extent that it is necessary to do so in order to avoid or mitigate the potential impact of any Compromise to the DCC Systems, temporarily suspend:

(a) in respect of a Party whose actions or Systems are giving rise to the actual or threatened Compromise:

(i) the provision (in whole or in part) of the Services to that Party;

(ii) the rights of that Party to receive (in whole or in part) the Services; and/or

(iii) the ability of that Party to use any DCC Gateway Connection; or

(b) in respect of an RDP whose actions or Systems are giving rise to the actual or threatened Compromise, the ability of that RDP to use any DCC Gateway Connection.

H10.3 Where the DCC commences any temporary suspension of the provision of Services or rights, or of the ability to use a DCC Gateway Connection in accordance with Section H10.2, it shall promptly (and in any event within 24 hours) notify the Panel of the suspension and the reasons for it, and shall provide the Panel with such information relating to the suspension as may be requested.

H10.4 Where the Panel receives a notification in accordance with Section H10.3, it shall promptly consider the circumstances of the suspension, and:

(a) shall either confirm the suspension, or determine that the suspension is to cease to have effect (in which case the suspended Services, rights or ability to use any DCC Gateway Connection shall be reinstated); and

(b) may in either case give such directions as it considers appropriate:

(i) to the DCC in relation to the continuing suspension or the reinstatement of the Services, rights or ability to use any DCC Gateway Connection (as the case may be); and/or

(ii) to the Party or RDP whose Services, rights or ability to use any DCC Gateway Connection were suspended by the DCC, for the purpose of remedying any actual or potential cause of Compromise to the DCC Systems or for preventing its recurrence.

H10.5 The DCC shall comply with any direction given to it by the Panel in accordance with Section H10.4, and shall provide such reasonable support and assistance to the Party or RDP whose Services, rights or ability to use any DCC Gateway Connection were suspended by the DCC as that Party or RDP may request for the purpose of remedying any actual or potential cause of Compromise to the DCC Systems or for preventing its recurrence.

H10.6 A Party shall comply with any direction given to it by the Panel in accordance with Section H10.4.

H10.7 Each Electricity Network Party and each Gas Network Party shall ensure that its RDP shall (when acting in its capacity as the Network Party's RDP) comply with any direction given to it by the Panel in accordance with Section H10.4.

H10.8 Where the DCC or any Party or RDP which is directly affected by a decision of the Panel made pursuant to Section H10.4 disagrees with that decision, it may refer the matter to the Authority for its determination, which shall be final and binding for the purposes of this Code.

The Business Continuity and Disaster Recovery Procedure

H10.9 Subject to Section H10.10, the DCC shall comply with the requirements of the Business Continuity and Disaster Recovery Procedure for the purposes of ensuring so far as reasonably practicable that:

(a) there is no significant disruption to the provision of any of the Services by the DCC; and

(b) where there is any such significant disruption, the provision of those Services is restored as soon as is reasonably practicable.

H10.10 Where, in the case of Disasters, taking a different course of action to following the BCDR Procedure would (in accordance with Good Industry Practice) be a more effective course of action in order to achieve the objectives set out in Section H10.9, then the DCC may take such steps to achieve such objectives (rather than complying with the BCDR Procedure). Where the DCC takes a course of action that does not comply with the BCDR Procedure, the DCC must inform the Panel as soon as possible thereafter of the steps taken and the reasons why the DCC considered that they were more effective.

Business Continuity and Disaster Recovery Tests

H10.11 The DCC shall (subject to any contrary provisions in the SEC Subsidiary Documents applying in relation to the SMETS1 SM WAN and/or the Systems of the SMETS1 Service Providers):

(a) from time to time, and at least once each year, carry out a Business Continuity and Disaster Recovery Test in order to assess whether the Business Continuity and Disaster Recovery Procedure remains suitable for achieving the objectives described at Section H10.9; and

(b) following any such test, report to the Panel and the Authority on the outcome of the test, and on any proposals made by the DCC in relation to the Business Continuity and Disaster Recovery Procedure having regard to that outcome.

H10.12 Each Party shall provide the DCC with any such assistance and co-operation as it may reasonably request for the purpose of carrying out a Business Continuity and Disaster Recovery Test and confirming the operation of the Business Continuity and Disaster Recovery Procedure.

H10.12A Before notifying the Parties of each Business Continuity and Disaster Recovery Test, the DCC shall consult with the Parties and the Panel regarding the Business Continuity and Disaster Recovery Test Schedule to ensure that (insofar as is reasonably practicable) the Business Continuity and Disaster Recovery Test is undertaken in such a way as to minimise any disruption to the provision of the Services (or any part of them). The DCC shall complete all necessary consultation prior to notifying Parties.

H10.12B The DCC shall notify each Party of its intention to carry out a Business Continuity and Disaster Recovery Test and provide each Party with a Business Continuity and Disaster Recovery Test Schedule at least 60 Working Days before the date on which such test is due to start. Where the DCC needs to amend the Business Continuity and Disaster Recovery Test Schedule following such notification and it is not reasonably practicable to give 60 Working Days' notice, it will provide such notice as far in advance as is reasonably practicable.

Business Continuity and Disaster Recovery Targets

H10.13 The DCC shall, on the occurrence of a Disaster (subject to any contrary provisions in the SEC Subsidiary Documents applying in relation to the SMETS1 SM WAN and/or the Systems of the SMETS1 Service Providers):

(a) take all reasonable steps to ensure that any and all affected Services are restored in accordance with the Target Resolution Time for a Major Incident;

(b) ensure that all affected Services are restored within eight hours of the occurrence of that Disaster (except in the case of a Disaster that directly affects a DCC Gateway Connection and where: (i) the DCC Gateway Party for that DCC Gateway Connection has not procured a backup DCC Gateway Connection; and (ii) the DCC can reasonably demonstrate that the Services could have been restored within eight hours if the DCC Gateway Party had procured a backup DCC Gateway Connection); and

(c) ensure in any event that Services are restored such that the loss of Data arising as a consequence of the Disaster is not in excess of that prescribed by the relevant Service Provider Performance Measures.

H11. PARSE AND CORRELATE SOFTWARE

Provision of Parse and Correlate Software

H11.1 On receipt of a request to do so from any person, the DCC shall supply to that person a copy of the most recently released version of computer software (the "**Parse and Correlate Software**") which:

(a) has the functionality specified in Section H11.2;

(b) has the characteristics specified in Section H11.3; and

(c) is provided in the format specified in Section H11.4.

H11.2 The functionality specified in this Section H11.2 is that the software must enable any User to:

(a) convert the relevant content of all Service Responses and Device Alerts (in each case only where generated from a Response or Alert originating from a SMETS2+ Device) into the format that is consistent with that set out in respect of them in the Message Mapping Catalogue; and

(b) confirm that the content of any Pre-Command is substantively identical to the content of its associated Critical Service Request.

H11.3 The characteristics specified in this Section H11.3 are that:

(a) the software is written using the Java programming language; and

(b) the software is capable of operating on the version of the Java Virtual Machine/Run-time Environment prevailing at the time at which the design of that version of the software was finalised.

H11.4 The format specified in this Section H11.4 is that the software:

(a) is provided as both:

(i) an executable file which includes everything required to enable the software to be installed on the systems of the person to whom it is provided in such a manner as not to have a material adverse effect on the operation of other software deployed within the same system environment; and

(ii) source software code.

(b) can be confirmed, on receipt by the person to whom it is provided:

(i) as having been provided by the DCC; and

(ii) as being authentic, such that any tampering with the software would be apparent.

Maintenance of the Parse and Correlate Software

H11.5 The DCC shall:

(a) maintain the Parse and Correlate Software supplied by it to any person so as to ensure that it at all times continues to have the functionality specified in Section H11.2; and

(b) for that purpose develop and release to such persons, where it is reasonably necessary from time to time, new versions of the Parse and Correlate Software which shall have the characteristics specified in Section H11.3 and be provided in the format specified in Section H11.4.

Development of the Parse and Correlate Software

H11.6 When proposing to develop any version of the Parse and Correlate Software, the DCC shall consult with Users, having regard in particular to their views in relation to:

(a) the need for a new version of the software;

(b) the potential impact of the proposed new version of the software on the security of the DCC Total System, User Systems and Smart Metering Systems;

(c) the design of the software generally; and

(d) the required operational performance of the proposed version of the software on a standard system configuration specified by the DCC for the purposes of the consultation.

H11.7 Following any consultation with Users, the DCC shall inform all Users of the design of the version of the Parse and Correlate Software that it intends to develop.

H11.8 Before supplying any version of the Parse and Correlate Software to any person, the DCC shall:

(a) ensure that that version of the software has been adequately tested for the purpose of ensuring that it satisfies the requirements of Sections H11.2 to H11.4;

(b) provide suitable opportunities for Acceptance Testing of that version of the software;

(c) take reasonable steps to ensure that any User who wishes to participate in that Acceptance Testing is able to do so; and

(d) ensure that the version of the software has been subject to a software code review, by an individual or organisation with the professional competence to carry out such a review, for the purpose of identifying any vulnerabilities in the code that were not intended as a feature of its design.

Provision of Support and Assistance to Users

H11.9 The DCC shall, having consulted with Users, determine two Application Servers in respect of which it will provide support for the executable file referred to in Section H11.4(a)(i).

H11.10 Any User may appeal to the Panel a decision of the DCC made under Section H11.9, in which case:

(a) the Panel shall determine the Application Servers in respect of which the DCC must provide support; and

(b) the determination of the Panel shall be final and binding for the purposes of this Code.

H11.11 The DCC shall make available to each person to whom any version of the Parse and Correlate Software is provided a copy of an installation guide and release notes relevant to that version.

H11.12 Requests by any User for the DCC to provide that User with further assistance in relation to its use or implementation of the Parse and Correlate Software shall be made in such format as the DCC may specify from time to time, and shall be submitted to the DCC. Following receipt of any such request (or purported request), the DCC shall:

(a) where the request is incomplete or the DCC reasonably requires further information in order to assess the request, notify the User that this is the case and provide reasonable assistance to the User in re-submitting its request;

(b) once the DCC has received all the information it reasonably requires in order to assess the request, confirm the reasonable terms upon which the DCC will provide the requested assistance (which terms may not be inconsistent with the provisions of this Code) and the Charges payable in respect of the same; and

(c) once the Party has agreed to such terms and to pay such Charges, provide the requested assistance to the User in accordance with such terms.

H11.13 Section H11.12 does not apply to the provision of assistance that is the responsibility of the DCC in accordance with the Incident Management Policy. The assistance referred to in Section H11.12 may include in particular assistance in respect of:

(a) the development and testing of, and the provision of support for, a version of the Parse and Correlate Software which is capable of operating on a version of the Java Virtual Machine/Run-time Environment other than that prevailing at the time at which the design of the most recently released version of the Parse and Correlate Software was finalised;

(b) the development and testing of, and the provision of support for, a version of the Parse and Correlate Software which meets any other User-specific requirements; and

(c) the provision, in respect of more than two Application Servers, of support for the executable file referred to in Section H11.4(a)(i).

Separation of Resources

H11.14 The DCC shall ensure that no staff or other resources of its own or of any third party which are directly used in the development of the Parse and Correlate Software are resources which are also used in the development or provision of the Transform functionality.

Right to Use the Parse and Correlate Software

H11.15 The DCC shall ensure that any person shall have the right to use the Parse and Correlate Software source software code on a non-proprietary and royalty-free basis, except insofar as royalties are due in respect of any Intellectual Property Rights the use of which is mandated by the Code.

H12. INTIMATE COMMUNICATIONS HUB INTERFACE SPECIFICATION

Maintenance of the ICHIS

H12.1 The DCC shall maintain the ICHIS and ensure that the ICHIS meets the requirements of Section H12.2 and H12.3. The ICHIS is not relevant to SMETS1 CHs.

H12.2 The requirements of this Section H12.2 are that the ICHIS describes a specification for the physical interface (including the electrical and data connection) between:

(a) the Communications Hub (which shall incorporate the male components of the physical interface); and

(b) either a Smart Meter or a Communications Hub Hot Shoe (which shall, in either case, incorporate the female components of the physical interface).

H12.3 The requirement of this Section H12.3 is that the specification described by the ICHIS only requires the use of tangible and intangible property (including physical components and Intellectual Property Rights) that is readily available on a reasonable and non-discriminatory basis.

Publication of the ICHIS

H12.4 The DCC shall publish the ICHIS on the DCC Website, and ensure that all persons are free to use the ICHIS without charge (whether for the purposes of this Code or otherwise); provided that the DCC shall limit its liability to persons other than the Parties on the same terms as apply in respect of the ICHIS under Section M2 (Limitations of Liability).

Consultation Regarding ICHIS

H12.5 The DCC shall keep the ICHIS under review to ascertain whether the ICHIS remains fit for the purposes envisaged by this Code. The DCC may from time to time at its discretion (and shall where directed to do so by the Panel) consult with Parties as to whether they consider that the ICHIS remains fit for the purposes envisaged by this Code.

H12.6 Following each consultation pursuant to Section H12.5, the DCC shall publish on the DCC Website (and notify all Parties of) a report on the outcome of such consultation, setting out:

(a) the process undertaken in respect of such consultation;

(b) whether (and, if so, how and from what implementation date) the DCC proposes to amend the ICHIS as a result of such consultation;

(c) a detailed summary of the consultation responses received from Parties, identifying in particular those responses that raised objections to the position adopted by the DCC;

(d) the DCC's rationale for the position it has adopted;

(e) the costs and expenses that are likely to arise as a result of the position adopted by the DCC (including the costs and expenses likely to arise as a result of any modifications that will be required to be made to Smart Meters, Communications Hubs and Communications Hub Hot Shoes); and

(f) the steps it has taken (including any testing or prototype development) to ensure that the ICHIS (if amended as proposed) remains fit for the purposes envisaged by this Code.

Referral to the Authority

H12.7 Within 10 Working Days following notification by the DCC to a Party of a report published in accordance with Section H12.6, that Party may refer the report to the Authority to consider whether the consultation to which that report relates was undertaken in accordance with the DCC's obligations under this Code or whether the notice period provided for implementation of the amendment was reasonable given the circumstances.

H12.8 Where the Authority determines that the relevant consultation was not undertaken in accordance with the DCC's obligations under this Code or that the notice period provided for implementation of the amendment was not reasonable given the circumstances, the DCC shall repeat the consultation and comply with any directions made by the Authority in respect of the same. Where the Authority determines both (where both of the following were referred to the Authority) or either (where only one of the following was so referred) that:

(a) the relevant consultation was undertaken in accordance with the DCC's obligations under this Code; and/or

(b) the notice period provided for implementation of the amendment was reasonable given the circumstances,

the consultation and proposed course of action shall stand.

Amendments to the ICHIS

H12.9 No amendment may be made to the ICHIS unless:

(a) the DCC has first undertaken such prototype development and testing in respect of the proposed amendment as the DCC reasonably considers necessary to ensure that the ICHIS is fit for the purposes envisaged by this Code;

(b) the DCC has first consulted with Parties regarding the proposed amendment and proposed date of implementation, published a report on the outcome of such consultation, and notified the Parties of such publication (all in accordance with Section H12.6); and

(c) such report has not been referred to the Authority in accordance with Section H12.7, or the Authority has determined both (where both of the following were so referred) or either (where only one of the following was so referred) that:

(i) the relevant consultation was undertaken in accordance with the DCC's obligations under this Code; and/or

(ii) the notice period provided for implementation of the amendment was reasonable given the circumstances.

H13. PERFORMANCE STANDARDS AND REPORTING

Code Performance Measures

H13.1 Each of the following performance measures constitute a Code Performance Measure (to which the following Target Service Level and Minimum Service Level will apply, measured over the following Performance Measurement Period):

No.	Code Performance Measure	Performance Measurement Period	Target Service Level	Minimum Service Level

1	Percentage of On-Demand Service Responses delivered within the applicable Target Response Time.	monthly	99%	96%
2	Percentage of Future-Dated Service Responses delivered within the applicable Target Response Time.	monthly	99%	96%
3	Percentage of Alerts delivered within the applicable Target Response Time (including the Alerts which are subject to Sections H3.14(i) and (j). Alerts consolidated in accordance with the Alert Management Mechanism will not be counted.	monthly	99%	96%
3A	For those Alerts which are subject to Section H3.14(i), percentage of Alerts delivered within the applicable Target Response Time.	monthly	As set out in the Power Outage & Restoration Alerts Delivery Management Document	As set out in the Power Outage & Restoration Alerts Delivery Managemen t Document
4	Percentage of Incidents which the DCC is responsible for resolving and which fall within Incident Category 1 or 2 that are resolved in accordance with the Incident Management Policy within the Target Resolution Time.	monthly	100%	85%
5	Percentage of Incidents, measured and reported as a separate Code Performance Measure for each of Incident Categories 3, 4 and 5, which the DCC is responsible for resolving that are resolved in accordance with the Incident Management Policy within the Target Resolution Time.	monthly	90%	80%
5A	Percentage of Incidents which fall within Incident Category 3, 4 or 5 that are recorded on the Incident Management Log and assigned to a resolver within the Target Initial Response Time.	monthly	90%	80%
6	Percentage of time (in minutes) during which each DCC Interface (excluding the one listed in paragraph (f) of the definition of DCC Interface) is available during the Target Availability Period. There shall be a separate Code Performance Measure for each combination of DCC Interface, Region and the two relevant times of day (the first such relevant time of day being Monday-Friday 08.00-20.00 and Saturday 08.00-12.00; the second being every other time). For this purpose, a DCC Interface is only considered to be available where it and the DCC Systems on which it relies are fully available, such that those persons which are intended to be able to use the DCC	monthly	99.5%	98%

	Interface can use the full functionality which is intended to be available to them.			
6A	Percentage of each of the Business Processes described in Section H13.1A which is delivered within the applicable Target Response Time. There shall be a separate Code Performance Measure for each combination of Business Processes and either Region (for SMETS2+) or SMETS1.	monthly	99%	96%

H13.1A The Business Processes referred to in Code Performance Measure 6A above are a combination of Service Reference Variants as set out in the table below. The percentage of each Business Process which is delivered within the Target Response Time shall be measured and calculated by reference to whether the messages that together comprise that Business Process were sent and received within the required Target Response Time. For this purpose, a Service Response will not be considered to have been received if the Service Response contains an error Response Code relating to a communications failure or timeout (E20 or E21).

Business Process	**Service Reference Variant**	**Description**	**SMETS1 applicable**
Install and Commission	8.11	Update HAN Device Log	Yes
	6.21	Request Handover of DCC Controlled Device (Update Supplier Certificates)	No
	8.1.1	Commission Device	Yes
	8.7.2	Join Service (Join GPF with GSME)	Yes
	6.20.1	Set Device Configuration (Import MPxN)	No
	1.1.1	Update Import Tariff (Primary Element)	Yes
	6.8	Update Device Configuration (Billing Calendar)	Yes
	8.14.1	Communications Hub Status Update Install Success	No
Change of Supplier (Gain)	6.23	Update Security Credentials (CoS)	Yes
	1.1.1	Update Import Tariff (Primary Element)	Yes
	6.8	Update Device Configuration (Billing Calendar)	Yes
Change of Tenancy	3.2	Restrict Access for Change of Tenancy	Yes
Tariff Updates	1.1.1	Update Import Tariff (Primary Element)	Yes
Pre-Payment	1.6	Update Payment Mode (Payment Mode = Prepayment)	Yes
	2.1	Update Prepay Configuration	Yes
	2.2	Top Up Device (Update Balance with positive value)	Yes
Security and Key Management	6.15.2	Update Security Credential (Device) – Credential Type = Digital Signature	No

	6.15.2	Update Security Credential (Device) – Credential Type = Key Agreement	No
	6.17	Issue Security Credentials – Credential Type = Digital Signature	No
	6.17	Issue Security Credentials – Credential Type = Key Agreement	No
Update Device Firmware	11.1	Update Firmware Note: In respect of SMETS2+ Devices the DCC must ensure that the associated firmware update has been delivered to all relevant Communications Hub Functions within five days of receipt of the Service Request.	No
	11.3	Activate Firmware (Individual SR for each GUID for firmware activation)	No
Logistics CH Ordering and Returns	8.14.3	Communications Hub Status Update – Fault Return	No
	8.14.4	Communications Hub Status Update – No Fault Return	No
Distribution Networks Post I&C Activity	6.15.1	Update Security Credentials (Update Network Operator Certificates)	Yes
	6.5	Update Device Configuration (Voltage)	Yes
	6.22	Configure Alert Behaviour (Update ENO Alter Configuration)	No
Meter Reads	4.6.1	Retrieve Import Daily Read Log	Yes
	4.6.2	Retrieve Export Daily Read Log	No
	4.8.1	Read Active Import Profile Data	Yes
	4.8.2	Read Reactive Import Profile Data	Yes
	4.8.3	Read Export Profile Data	Yes
	4.10	Read Network Data	Yes
	4.17	Retrieve Daily Consumption Log	No

Note, where the response for the 'Update Security Credentials (CoS)' Service Request erroneously reports a failure, the presence of subsequent Critical and Non-Critical Service Requests sent by the gaining supplier will be used as an indicator of success.

Service Provider Performance Measures

H13.2 The DCC may modify the Reported List of Service Provider Performance Measures where it has:

(a) undertaken reasonable consultation with the Parties regarding the proposed modification;

(b) given due consideration to, and taken into account, any consultation responses received; and

(c) provided to the Panel, the Parties, the Authority and (on request) the Secretary of State a statement of its reasons for the modification together with copies of any consultation responses received, and as soon as reasonably practicable following any such modification, the DCC shall provide an up-to-date copy of the Reported List of Service Provider Performance Measures to the Panel, the Parties, the Authority and (on request) the Secretary of State.

H13.3 Prior to agreeing any changes to the DCC Service Provider Contracts that will alter the Service Provider Performance Measures, the DCC shall:

(a) undertake reasonable consultation with the Panel and Parties regarding such changes;

(b) give due consideration to, and take into account, any consultation responses received; and

(c) provide to the Panel, the Parties, the Authority and (on request) the Secretary of State a statement of its reasons for proposing to agree such changes.

Reporting

H13.4 The DCC shall, within 25 Working Days following the end of each Performance Measurement Period, produce a report setting out the Service Levels achieved in respect of each Performance Measure. Such report must identify:

(a) those Performance Measures (if any) for which the Service Level was less than the Target Service Level and/or the Minimum Service Level;

(b) where a Service Level is less than the Target Service Level, the reason for the Service Level achieved;

(c) where a Service Level is less than the Minimum Service Level, the steps the DCC is taking to prevent the re-occurrence or continuation of the reason for the Service Level achieved; and

(d) any anticipated reductions in the DCC's Internal Costs and/or External Costs (as both such expressions are defined in the DCC Licence) arising as a consequence of the DCC Service Providers failing to achieve the Target Service Levels in respect of the Service Provider Performance Measures.

H13.5 A copy of the report produced pursuant to Section H13.4:

(a) shall be provided by DCC, immediately following its production, to the Panel, the Parties, the Authority and (on request) the Secretary of State; and

(b) may be provided by the Panel, at its discretion, to any other person.

Report on Performance Indicators

H13.5A At the same time as the report required under Section H13.4, the DCC shall also report on its performance against the Performance Indicators for the same period.

H13.5B The Panel shall establish and periodically review, in consultation with the Parties and the Authority, a document (to be known as the DCC Performance Indicators Document) which lists the reasonable service metrics which are to constitute the Performance Indicators, and which are therefore to be measured and reported on by the DCC. The DCC Performance Indicators Document shall include the Performance Indicators described in Section H13.5C and shall require these to be included in the report required under Section H13.5A and may request other individual Performance Indicator(s) to be included in the report, including:

(a) graphs of daily performance in respect of delivery of each of the Business Processes;

(b) monthly median figures for performance in respect of delivery of each of the Business Processes;

(c) the total number of each of the Business Processes delivered each month;

(d) for each DCC Interface separately, the average amount of downtime per Incident; and

(e) for each DCC Interface separately, the mean amount of time between Incidents.

H13.5C When looked at on an Alert type basis (as opposed to when aggregated with other Alert types pursuant to row 3 of the table in Section H13.1), the performance of the Alerts which are subject to Section H3.14(j) against the relevant Target Response Time set out in the DCC's Power Outage & Restoration Alerts Delivery Management Document shall be Performance Indicators.

Performance Measurement Methodology

H13.6 The DCC shall:

(a) establish and periodically review the Performance Measurement Methodology in accordance with Good Industry Practice and in consultation with the Panel, the Parties and the Authority;

(b) seek approval from the Panel for any proposed changes that the DCC wishes to make to the Performance Measurement Methodology; and

(c) as soon as reasonably practicable following any modification which the Panel approves, provide an up to date copy of the Performance Measurement Methodology to the Panel, the Parties, the Authority and (on request) the Secretary of State.

Customer Analytics Reporting

H13.6A The DCC Shall:

(a) establish and periodically review the Customer Analytics Reporting Methodology and Guidance Document (including such reviews as the Panel may request), in consultation with the Panel and Users;

(b) seek approval from the Panel for any proposed changes that the DCC wishes to make to the Customer Analytics Reporting Methodology and Guidance Document; and

(c) make the Customer Analytics Reporting Methodology and Guidance Document available to the Panel and the Users.

H13.6B The Customer Analytics Reporting Methodology and Guidance Document must:

(a) set out the requirements that the DCC will undertake:

(b) provide performance metrics for Services, and must provide each User with details of the performance achieved in respect of that User against those metrics, together with details of the performance achieved in respect of other Users in the same User Role on an anonymised, industry-wide basis; and

(c) provide guidance to Users regarding the provision of Customer Analytics Reporting by the DCC.

H13.6C The DCC shall, within 10 working days following the end of each month, provide the Users with the Customer Analytics Reporting for the prior month.

H13.6D Clauses 13.6A to 13.6C shall only apply from 31 December 2024.

OPR Exceptional Events

H13.7 Sections H13.7 to H13.14 shall apply only to the extent that the OPR Reporting established under the DCC Licence applies by reference to reporting under this Code. OPR Exceptional Events shall not apply in respect of Performance Measure reporting under Section H13.4.

H13.8 For the purposes of OPR Reporting, in measuring performance for each Performance Measure, the DCC shall exclude from the Service Level calculation any and all instances of delayed or non-performance for which the DCC has relief for an OPR Exceptional Event by virtue of Section H13.12.

H13.9 The DCC may claim relief for the purposes of OPR Reporting in respect of the Performance Measures to the extent this is due to OPR Exceptional Events. Where the DCC also wishes to claim relief in respect of its obligations under this Code, the DCC must also separately claim relief for Services FM under Section M3 (Services FM and Force Majeure).

H13.10 The DCC cannot claim an OPR Exceptional Event has occurred:

(a) in relation to any wilful act, neglect or failure to take reasonable precautions against the relevant OPR Exceptional Event by the DCC or its servants, agents, employees or contractors (including the DCC Service Providers);

(b) in relation to any circumstances resulting from a failure or delay by any other person in the performance of that other person's obligations under a contract with the DCC other than this Code (unless that other person is itself prevented from or delayed in complying with its obligations as a result of OPR Exceptional Events); and/or

(c) as a result of any shortage of labour, material or other resources unless caused by circumstances which are themselves OPR Exceptional Events,

and in any event, the DCC shall not be entitled to relief for the purposes of OPR Reporting if and to the extent that it is required to comply with the BCDR Procedure in accordance with Sections H10.9 and H10.10 (the Business Continuity and Disaster Recovery Procedure) but has failed to do so (unless this failure is also due to OPR Exceptional Events affecting the operation of the BCDR Procedure).

H13.11 The DCC shall, as soon as reasonably practicable (and in any event within five (5) days of the occurrence of the OPR Exceptional Event), give to the Users that were due to receive the affected Services and to the Panel full details of the OPR Exceptional Event and any relief for the purposes of OPR Reporting which the DCC wishes to claim in connection with the OPR Exceptional Event.

H13.12 The DCC shall be entitled to relief for the purposes of OPR Reporting in respect of OPR Exceptional Events to the extent that the Panel agrees following consultation with any relevant Sub-Committee that the requirements of Sections H13.9 and H13.10 are met, and that:

(a) the DCC could not have avoided the occurrence of the OPR Exceptional Event (or its consequences or likely consequences) by taking steps which the DCC was required to take (or procure) under this Code and any Bilateral Agreement or might reasonably be expected to have taken;

(b) the OPR Exceptional Event directly caused the non-performance of the Services for which relief is claimed;

(c) the time lost and/or relief from the obligations under this Code and any Bilateral Agreement claimed by the DCC could not reasonably be expected to be mitigated or recovered by the DCC acting in accordance with Good Industry Practice; and

(d) the DCC is taking all steps in accordance with Good Industry Practice to overcome or minimise the consequences of the OPR Exceptional Event on the performance of the Services.

H13.13 The Panel shall reach a determination as to whether the DCC is entitled to relief for the purposes of OPR Reporting in respect of an OPR Exceptional Event in accordance with Section H13.12 within 10 Working Days after the DCC notifies the Panel of the OPR Exceptional Event under Section H13.11.

H13.14 The DCC shall notify the affected Users and the Panel as soon as reasonably practicable after the OPR Exceptional Event ceases or no longer causes the DCC to be unable to comply with its obligations under this Code and/or any Bilateral Agreement in respect of the Services.

H14. TESTING SERVICES

General Testing Requirements

H14.1 The DCC shall provide the following testing services (the "**Testing Services**"):

(a) User Entry Process Tests;

(b) SMKI and Repository Entry Process Tests;

(c) Device and User System Tests;

(d) Modification Proposal implementation testing (as described in Section H14.34);

(e) DCC Internal Systems change testing (as described in Section H14.36);

(f) RDP Entry Process Tests;

(g) SMETS1 Pending Product Combinations Tests;

(h) RF Noise Testing;

(i) Interoperability and Innovation Events;

(j) GFI Testing;

(k) Wired Instrumented Test Communications Hubs; and

(l) DCC Boxed.

H14.2 The DCC shall make the Testing Services available, and shall provide the Testing Services:

(a) in accordance with the Enduring Testing Approach Document and Good Industry Practice; and

(b) between 08:00 hours and 18.00 hours Monday to Friday, and at any other time that it is reasonably practicable to do so (including where any DCC Service Provider has agreed to provide services at such time).

H14.3 The DCC shall act reasonably in relation to its provision of the Testing Services and shall facilitate the completion (in a timely manner) of tests pursuant to the Testing Services by each such person which is entitled to do so in accordance with this Section H14. Each Testing Participant shall comply with the Enduring Testing Approach Document with respect to the relevant Testing Services. The DCC shall publish on the DCC Website a guide for Testing Participants describing which persons are eligible for which Testing Services, and on what basis (including any applicable Charges).

H14.4 To the extent it is reasonably practicable to do so, the DCC shall allow persons who are eligible to undertake tests pursuant to the Testing Services to undertake those tests concurrently, or shall (otherwise) determine, in a non-discriminatory manner, the order in which such persons will be allowed to undertake such tests. Where any Testing Participant disputes the order in which persons are allowed to undertake tests pursuant to this Section H14.4, then the Testing Participant may refer the matter to the Panel. Where the DCC or any Testing Participant wishes to do so, it may refer the Panel's decision on such matter to the Authority for its determination (which shall be final and binding for the purposes of this Code).

H14.5 Each Party which undertakes tests pursuant to the Testing Services shall do so in accordance with Good Industry Practice. To the extent that such tests involve a Party accessing the DCC's premises, the Party shall do so in compliance with the site rules and reasonable instructions of the DCC.

H14.6 The DCC shall be liable for any loss of or damage to the equipment of Testing Participants (fair wear and tear excepted) that occurs while such equipment is within the DCC's possession or control pursuant to the Testing Services; save to the extent that such loss or damage is caused by a breach of this Code (or the equivalent agreement under Section H14.7) by the Testing Participant.

H14.7 Where (in accordance with this Section H14) a person that is not a Party is eligible to undertake a category of Testing Services as a Testing Participant, the DCC shall not provide those Testing Services to that person unless it is bound by an agreement entered into with the DCC pursuant to this Section H14.7. Where a person who is a Testing Participant (but not a Party) requests a Testing Service, the DCC shall offer terms upon which such Testing Service will be provided. Such offer shall be provided as soon as reasonably practicable after receipt of the request, and shall be based on the Specimen Enabling Services Agreement (subject only to such variations from such specimen form as are reasonable in the circumstances).

General: Forecasting

H14.8 Each Testing Participant shall provide the DCC with as much prior notice as is reasonably practicable of that Testing Participant's intention to use any of the following Testing Services: User Entry Process Tests, SMKI and Repository Entry Process Tests, Device and User System Tests, SMETS1 Pending Product Combinations Tests and RF Noise Testing.

General: Systems and Devices

H14.9 The DCC shall provide such facilities as are reasonably required in relation to the Testing Services, including providing:

(a) for access to the Testing Services either at physical test laboratories and/or remotely;

(b) a reasonable number of Test Communications Hubs for use by Testing Participants at the DCC's physical test laboratories which represent each and every combination of HAN Variant and WAN Variant; and

(c) a reasonable number of Devices (other than SMETS2+ Communications Hubs) for use by Testing Participants at the DCC's physical test laboratories, which Devices are to be:

(i) in the case of SMETS1 Devices as further described or set out in the Enduring Testing Approach Document; or

(ii) except for SMETS1 Devices, such Device Models as the Panel approves from time to time (provided that, where Test Stubs (or other alternative arrangements) were used then such Tests Stubs (or other alternative arrangements) will be used in place of Devices until the DCC agrees with the Panel which Device Models to use).

H14.10 Without prejudice to Sections H14.9(b) and (c), the DCC shall allow Testing Participants to use Devices they have procured themselves when using the Testing Services. The DCC shall make storage facilities available at the DCC's physical test laboratories for the temporary storage by Testing Participants of such Devices (for no more than 30 days before and no more than 30 days after completion of the Testing Service for which such Devices may be expected to be used). The DCC shall ensure that such storage facilities are secure and only capable of access by persons authorised by the relevant Testing Participant.

H14.10A The DCC may require a Testing Participant to remove its Devices from a DCC physical test laboratory in accordance with the requirements set out in the Enduring Testing Approach Document. Any dispute between the DCC and a Testing Participant regarding the removal of such Devices (or the right to re-commence testing) may be referred to the Panel for its determination (which determination shall be final and binding for the purposes of this Code).

General: SMKI Test Certificates

H14.11 The following shall apply in relation to Test Certificates:

(a) the DCC shall, in accordance with the Enduring Testing Approach Document, issue and make available to Testing Participants copies of such Test Certificates as are reasonably necessary for the purposes of the Testing Participants undertaking Testing Services;

(b) the DCC shall only use Test Certificates for the purposes envisaged by this Section H14.11 (and shall not use actual Certificates when providing the Testing Services, except to such extent as is approved, and subject to any conditions imposed, by the SMKI PMA);

(c) each Testing Participant to which Test Certificates are made available pursuant to this Section H14.11 shall only use those Test Certificates for the purposes for which such Test Certificates are made available (and shall not use actual Certificates when undertaking the tests referred to in this Section H14.11);

(d) each Testing Participant to which Test Certificates are made available pursuant to this Section H14.11 shall be entitled to make those certificates available to others provided that such others only use them for the purposes for which such certificates were made available to the Testing Participant;

(e) DCC shall ensure that the Test Certificates are clearly distinguishable from actual Certificates;

(f) the DCC shall act in accordance with Good Industry Practice in providing the Test Certificates;

(g) each Testing Participant shall act in accordance with Good Industry Practice in using the Test Certificates; and

(h) each Testing Participant hereby, subject to Section M2.1 (Unlimited Liabilities):

(i) waives all rights, remedies and claims it would otherwise have (whether for breach of contract, in tort or delict or otherwise) against the DCC in respect of the Test Certificates;

(ii) undertakes not to bring any claim against the DCC in respect of the Test Certificates; and

(iii) where it makes the Test Certificates available to others, undertakes to ensure that no such others bring any claim against the DCC in respect of such Test Certificates.

User Entry Process Tests

H14.12 Parties seeking to become Users in accordance with Section H1 (User Entry Process) are entitled to undertake User Entry Process Tests.

H14.13 In respect of a Party seeking to become eligible as a User in a particular User Role, the purpose of the User Entry Process Tests is to test the capability of that Party and the Party's Systems to interoperate with the DCC and the DCC System, to the extent necessary in order that the Party:

(a) has established a connection to the DCC User Interface via the Party's chosen DCC Gateway Connection;

(b) can use the DCC User Interface for the purposes set out in Section H3.3 (Communications to be sent via DCC User Interface) in respect of the Services for which Users in that User Role are eligible; and

(c) can use the Self-Service Interface for the purposes set out in Section H8 (Service Management, Self-Service Interface and Service Desk).

H14.14 The User Entry Process Tests will:

(a) test the sending of communications from the proposed User System via the DCC System to be received by Devices and from Devices via the DCC System to be received by the proposed User System, recognising that such tests may involve a simulation of those Systems rather than the actual Systems;

(b) be undertaken in accordance with the Common Test Scenarios Document; and

(c) be undertaken using Devices selected and provided by the DCC as referred to in Sections H14.9(b) and (c).

H14.15 Only Parties who the DCC considers meet any entry requirements (for a particular User Role) set out in the Common Test Scenarios Document shall be entitled to undertake the User Entry Process Tests for that User Role.

H14.16 Where the DCC is not satisfied that a Party meets such entry requirements (for a particular User Role), that Party may refer the matter to the Panel for its determination. Where the Party disagrees with any such determination of the Panel, then the Party may refer the matter to the Authority for its determination (which shall be final and binding for the purposes of this Code).

H14.17 Each Party seeking to undertake the User Entry Process Tests shall develop its own test scripts and demonstrate how those test scripts meet the requirements of the relevant scenarios set out in the Common Test Scenarios Document. Each Party shall obtain the DCC’s approval that such test scripts meet those requirements before the User Entry Process Tests can commence. Any disputes regarding the approval of such test scripts may be referred to the Panel for determination (which determination shall be final and binding for the purposes of this Code).

H14.18 Each Party will have the right to determine the sequencing of the tests that comprise the User Entry Process Tests; save to the extent that a particular sequence is mandated in the Common Test Scenarios Document.

H14.18A The DCC or the Party undertaking the User Entry Process Tests may suspend testing in accordance with the requirements set out in the Common Test Scenarios Document. Any dispute between the DCC and a Party regarding the suspension (or consequent resumption) of such testing may be referred to the Panel for its determination. Where the DCC or the Party disagrees with any such determination of the Panel, then the DCC or the Party may refer the matter to the Authority for its determination (which determination shall be final and binding for the purposes of this Code).

H14.19 A Party will have successfully completed the User Entry Process Tests (for a particular User Role), once the DCC considers that the Party has demonstrated that it has satisfied the requirements set out in the Common Test Scenarios Document for that User Role. Where requested by a Party, the DCC shall provide written confirmation to the Party confirming whether or not the DCC considers that the Party has successfully completed the User Entry Process Tests (for a particular User Role).

H14.20 Where Systems have been proven to meet the requirements of this Code as part of one Party's successful completion of the User Entry Process Tests or tests under Section H14.32 that are equivalent to all or part of the User Entry Process Tests (and where the substance of the relevant part of the User Entry Process Tests have not changed in the interim), then:

(a) any Party that has use of those Systems shall be entitled to submit proof to the DCC that this is the case when seeking to meet any applicable entry and/or exit requirements set out in the Common Test Scenarios Document; and

(b) the DCC shall take into account such proof when considering whether such Party meets such entry and/or exit requirements.

H14.21 Where the DCC is not satisfied that a Party has successfully completed the User Entry Process Tests (for a particular User Role), that Party may refer the matter to the Panel for its determination. Where the Party disagrees with any such determination of the Panel, then the Party may refer the matter to the Authority for its determination (which shall be final and binding for the purposes of this Code).

SMKI and Repository Entry Process Tests

H14.22 Each Party or Registration Data Provider seeking to complete the entry process described in Section L7 (SMKI and Repository Entry Process Tests) is entitled to undertake the SMKI and Repository Entry Process Tests to become either or both of:

(a) an Authorised Subscriber under either or both of the Organisation Certificate Policy and/or the Device Certificate Policy; and/or

(b) eligible to access the SMKI Repository.

H14.23 The SMKI and Repository Entry Process Tests will be undertaken in accordance with the SMKI and Repository Test Scenarios Document.

H14.24 A Testing Participant seeking to undertake the SMKI and Repository Entry Process Tests for the purposes of either or both of Section H14.22(a) and/or (b) shall notify the DCC of the purposes for which it is undertaking those tests. Only Testing Participants that meet any applicable entry requirements set out in the SMKI and Repository Tests Scenarios Document shall be entitled to undertake those SMKI and Repository Entry Process Tests for the purposes described in Section H14.22(a) and/or (b).

H14.25 Where the DCC is not satisfied that a Testing Participant meets such entry requirements, that Testing Participant may refer the matter to the Panel for its determination. Where the Testing Participant disagrees with any such determination of the Panel, then the Testing Participant may refer the matter to the Authority for its determination (which shall be final and binding for the purposes of this Code).

H14.26 Each Testing Participant seeking to undertake the SMKI and Repository Entry Process Tests shall develop its own test scripts and demonstrate how those test scripts meet the requirements of the relevant scenarios set out in the SMKI and Repository Tests Scenarios Document (for the purposes described in Section H14.22(a) and/or (b), as applicable). Each Testing Participant shall obtain the DCC's approval that such test scripts meet those requirements before the SMKI and Repository Entry Process Tests can commence. Any disputes regarding the approval of such test scripts may be referred to the Panel for determination (which determination shall be final and binding for the purposes of this Code).

H14.27 Each Testing Participant seeking to undertake the tests will have the right to determine the sequencing of the tests that comprise the SMKI and Repository Entry Process Tests; save to the extent that a particular sequence is mandated in the SMKI and Repository Tests Scenarios Document.

H14.27A The DCC or the Testing Participant undertaking the SMKI and Repository Entry Process Tests may suspend testing in accordance with the requirements set out in the SMKI and Repository Test Scenarios Document. Any dispute between the DCC and a Testing Participant regarding the suspension (or consequent resumption) of such testing may be referred to the Panel for its determination. Where the DCC or the Testing Participant disagrees with any such determination of the Panel, then the DCC or the Testing Participant may refer the matter to the Authority for its determination (which determination shall be final and binding for the purposes of this Code).

H14.28 A Testing Participant will have successfully completed the SMKI and Repository Entry Process Tests (for the purposes described in Section H14.22(a) and/or (b), as applicable), once the DCC considers that the Testing Participant has demonstrated that it has satisfied the requirements set out in the SMKI and Repository Tests Scenarios Document for those purposes. Where requested by a Testing Participant, the DCC shall provide written confirmation to the Testing Participant confirming whether or not the DCC considers that the Testing Participant has successfully completed the SMKI and Repository Entry Process Tests (for the purposes described in Section H14.22(a) and/or (b), as applicable).

H14.29 Where Systems have been proven to meet the requirements of this Code as part of one Testing Participant's successful completion of the SMKI and Repository Entry Process Tests or tests under Section H14.32 that are equivalent to all or part of the SMKI and Repository Entry Process Tests (and where the substance of the relevant part of the SMKI and Repository Entry Process Tests have not changed in the interim), then:

(a) any Testing Participant that has use of those Systems shall be entitled to submit proof to the DCC that this is the case when seeking to meet any applicable entry and/or exit requirements set out in the SMKI and Repository Tests Scenarios Document; and

(b) the DCC shall take into account such proof when considering whether such Testing Participant meets such entry and/or exit requirements.

H14.30 Where the DCC is not satisfied that a Testing Participant has successfully completed the SMKI and Repository Entry Process Tests (for the purposes described in Section H14.22(a) and/or (b), as applicable), that Testing Participant may refer the matter to the Panel for its determination. Where the Testing Participant disagrees with any such determination of the Panel, then the Testing Participant may refer the matter to the Authority for its determination (which shall be final and binding for the purposes of this Code).

Device and User System Tests

H14.31 This Section H14.31 shall only apply in respect of SMETS1 Devices from 31 August 2018 or any such later date as the Secretary of State may direct further to a recommendation from the DCC to the Secretary of State following a consultation on a proposed date by the DCC with all SEC Parties and the SEC Panel. The DCC shall provide a service to enable Testing Participants:

(a) to test the interoperability of SMETS2+ Devices (other than those comprising Communications Hubs) with the DCC Systems and with the Test Communications Hubs provided as part of the Testing Services, such that those Devices are able to respond to Commands received from or via the DCC in accordance with the requirements defined in the GB Companion Specification;

(b) to test the interoperability of SMETS1 Devices with the DCC Systems, such that those Devices are able to respond to Instructions received from or via the DCC such that the necessary Equivalent Steps are taken (provided that such service need only be provided by the DCC in respect of combinations of SMETS1 Device Models that are listed on the SMETS1 Eligible Product Combinations);

(c) to test the interoperability of User Systems with the DCC Systems, including via the DCC User Interface and the Self-Service Interface;

(d) to test simultaneously the interoperability of User Systems and SMETS2+ Devices (other than those comprising Communications Hubs) with the DCC Systems and with the Test Communications Hubs provided as part of the Testing Services; and

(e) to test simultaneously the interoperability of User Systems and SMETS1 Devices (excluding combinations of SMETS1 Devices that are not listed on the SMETS1 Eligible Product Combinations) with the DCC Systems,

which Testing Services, except in respect of (c) above, shall (subject to the Testing Participant agreeing to pay any applicable Charges, as further described in the Enduring Testing Approach Document) include the provision of a connection to a simulation of the SMETS2+ SM WAN for the purpose of such tests as further described in the Enduring Testing Approach Document (save to the extent the connection is required where the DCC is relieved from its obligation to provide Communication Services pursuant to the Statement of Service Exemptions). For the avoidance of doubt, the DCC shall not be obliged by this Section H14.31 to provide a connection to a simulation of the SMETS1 SM WAN. References to particular Systems in this Section H14.31may include a simulation of those Systems (rather than the actual Systems).

H14.32 Each Party is eligible to undertake Device and User System Tests. Any Manufacturer (whether or not a Party) is eligible to undertake those Device and User System Tests described in Section H14.31(a) and (b); provided that, in the case of any such tests that require the use of a DCC Gateway Connection, the Manufacturer must be a Party. Any person providing (or seeking to provide) goods or services to Parties or Manufacturers in respect of Devices is eligible to undertake those Device and User System Tests described in Section H14.31(a) and (b); provided that, in the case of any such tests that require the use of a DCC Gateway Connection, the person must be a Party. A Party undertaking the Device and User System Tests described in Section H14.31(c) is entitled to undertake tests equivalent to any or all of the User Entry Process Tests and SMKI and Repository Entry Process Tests, in respect of which:

(a) the DCC shall, at the Party's request, assess whether the test results would meet the requirements of all or part of the applicable User Entry Process Tests and/or SMKI and Repository Entry Process Tests;

(b) the DCC shall, at the Party's request, provide a written statement confirming the DCC's assessment of whether the test results would meet the requirements of all or part of the applicable tests; and

(c) the Party may, where it disputes the DCC's assessment, refer the matter to the Panel for its determination (which shall be final and binding for the purposes of this Code).

H14.33 The DCC shall, on request by a Testing Participant, take all reasonable steps to offer additional support to that Testing Participant (subject to such Testing Participant agreeing to pay any applicable Charges) in understanding and resolving issues associated with:

(a) the DCC Total System and the results of such Testing Participant's Device and User System Tests;

(b) where the Testing Participant is a Party, the Systems of the Testing Participant that are (or are intended to be) User Systems; and/or

(c) communications between the DCC and any Device or between Devices which comprise (or which the Testing Participant intends will comprise) a Smart Metering System.

H14.33A The additional Testing Services provided for in Section H14.33 are without prejudice to the DCC's obligations in respect of Testing Issues, Incidents and Problems.

Modification Implementation Testing

H14.34 Where an approved Modification Proposal provides for the DCC to provide testing services as part of the Modification Proposal's implementation, then such testing shall be undertaken as a Testing Service pursuant to this Section H14.34.

H14.35 The Parties which are eligible, or obliged, to participate in such testing shall be determined in accordance with Section D (Modification Process), and either set out in this Code or established via a process set out in this Code.

DCC Internal System Change Testing

H14.36 Where, pursuant to Section H8.8 (DCC Internal Systems Changes), a Party or an RDP is involved in testing of changes to the DCC Internal Systems, then such testing shall not be subject to the requirements of Section H14.3, Section H14.4 and Sections H14.6 to H14.11 (inclusive), but such Party or RDP may nevertheless raise a Testing Issue in respect of the tests (and the references to Testing Participant in Sections H14.37 to H14.44 shall be interpreted accordingly).

SMETS1 Pending Product Combinations Tests

H14.36A This Section H14.36A shall only apply in respect of SMETS1 Devices from 31 August 2018 or any such later date as the Secretary of State may direct further to a recommendation from the DCC to the Secretary of State following a consultation on a proposed date by the DCC with all SEC Parties and the SEC Panel. The DCC shall provide services (the "**SMETS1 Pending Product Combinations Tests**") whereby a Party or a Manufacturer (being the relevant Testing Participant) can from time to time request that the DCC determines whether or not testing is required and, where it determines that testing is required, tests one or more combinations of SMETS1 Device Models and communication services provider that are not at that time listed on the SMETS1 Eligible Product Combinations in order to demonstrate whether the DCC is able to successfully process SMETS1 Service Requests and relevant SMETS1 Alerts in respect of them (subject to Section H14.36C(c)).

H14.36B Where requested in accordance with Section H14.36A, the DCC shall undertake, and facilitate the Testing Participant's participation in, the SMETS1 Pending Product Combinations Tests in respect of the requested combination(s) of SMETS1 Device Models as soon as reasonably practicable. The DCC shall then notify the relevant Testing Participant whether the DCC is able to successfully process SMETS1 Service Requests and relevant SMETS1 Alerts in respect of them, without needing to make material changes to the DCC Systems and/or modifications to this Code.

H14.36C Where the DCC notifies a Testing Participant that the DCC is not able to successfully process SMETS1 Service Requests and relevant SMETS1 Alerts in respect of a combination of SMETS1 Device Models without needing to make material changes to the DCC Systems and/or modifications to this Code, then the DCC shall:

(a) provide the relevant Testing Participant with reasonable details of the reasons why the DCC is not able to do so, and of the changes to the DCC Systems and/or modifications to this Code which would be required in order to enable the DCC to do so (in each case, to the extent that the DCC has been able to identify such reasons and changes and/or modifications, having taken reasonable steps to identify them);

(b) provide the relevant Testing Participant with such reasonable support as they may request in understanding the issues identified by the DCC;

(c) not be obliged to provide SMETS1 Pending Product Combinations Tests to the same Testing Participant in respect of the same combination of SMETS1 Device Models unless and until the relevant changes have been made to the DCC System and/or the relevant modifications have been made to this Code; and

(d) make available in accordance with the Enduring Testing Approach Document such details regarding the relevant combination of SMETS1 Device Models as is required in accordance with the Enduring Testing Approach Document.

H14.36D Where the DCC is able to successfully process SMETS1 Service Requests and relevant SMETS1 Alerts in respect of a combination of SMETS1 Device Models without needing to make material changes to the DCC Systems and/or modifications to this Code, then the DCC shall add that combination of Device Models to the SMETS1 Eligible Product Combinations.

H14.36E The DCC and the relevant Testing Participant in respect of the SMETS1 Pending Product Combinations Tests shall comply with any and all additional obligations concerning SMETS1 Pending Product Combinations Tests set out in the Enduring Testing Approach Document.

General: Testing Issue Resolution Process

H14.37 Each Testing Participant undertaking tests pursuant to this Section H14 is entitled to raise a Testing Issue in respect of those tests. Each Testing Participant shall take reasonable steps to diagnose and resolve a Testing Issue before raising it in accordance with this Section H14.

H14.38 A Testing Participant that wishes to raise a Testing Issue shall raise it with the relevant DCC Service Provider (as identified by the DCC from time to time) in accordance with a reasonable and not unduly discriminatory procedure, which is to be established by the DCC and provided to the Panel from time to time (which the Panel shall publish on the Website).

H14.39 Where a Testing Participant raises a Testing Issue, the DCC shall ensure that the relevant DCC Service Provider shall (as soon as reasonably practicable thereafter):

(a) determine the severity level and priority status of the Testing Issue;

(b) inform the Testing Participant of a reasonable timetable for resolution of the Testing Issue consistent with its severity level and priority status; and

(c) provide its determination (in accordance with such timetable) to the Testing Participant on the actions (if any) to be taken to resolve the Testing Issue.

H14.40 Pursuant to H14.39, the DCC shall share with categories of Testing Participant any information (provided that the identities of the Testing Participant and, where relevant, the Device's Manufacturer are anonymised) relating to the Testing Issue which is likely to be of use to those categories of Testing Participants (provided that no such information should be shared to the extent it poses a risk of Compromise to the DCC Total System, User Systems, RDP Systems and/or Devices).

H14.41 Where a Testing Participant is dissatisfied with any of the determinations under Section H14.39 (or the speed with which any such determination is made), the Testing Participant may refer the matter to the DCC. On such a referral to the DCC, the DCC shall (as soon as reasonably practicable thereafter):

(a) consult with the Testing Participant and any other person as the DCC considers appropriate;

(b) either, depending on the subject matter of the disagreement:

(i) direct the DCC Service Provider to more quickly provide its determination of the matters set out in Section H14.39(a), (b) and/or (c); or

(ii) make the DCC's own determination of the matters set out in Section H14.39(a), (b) and/or (c);

(c) notify the Panel of the DCC's direction or determination under (b) above; and

(d) share with categories of Testing Participant any information (provided that the identities of the Testing Participant and, where relevant, the Device's Manufacturer are anonymised) relating to the Testing Issue which is likely to be of use to those categories of Testing Participants (provided that no such information should be shared to the extent it poses a risk of Compromise to the DCC Total System, User Systems, RDP Systems and/or Devices).

H14.42 Where the Testing Participant (or any Party) disagrees with the DCC's determination pursuant to Section H14.41 of the matters set out at Section H14.39(c) (but not otherwise), then the Testing Participant (or Party) may request that the DCC refers the matter to the Panel for its consideration (provided that the identities of the Testing Participant and, where relevant, the Device's Manufacturer are anonymised).

H14.43 Where a matter is referred to the Panel for its consideration pursuant to Section H14.42, the Panel shall consider the matter further to decide upon the actions (if any) to be taken to resolve the Testing Issue. Where the Panel considers the matter further, it may conduct such further consultation as it considers appropriate before making such a decision. Such a decision may include a decision that:

(a) an aspect of the Code could be amended to better facilitate achievement of the SEC Objectives;

(b) an aspect of the DCC Systems is inconsistent with the requirements of this Code;

(c) an aspect of one or more Devices is inconsistent with the requirements of this Code; or

(d) an aspect of the User Systems or the RDP Systems is inconsistent with the requirements of this Code.

H14.44 The Panel shall publish each of its decisions under Section H14.43 on the Website; provided that the identities of the Testing Participant and (where relevant) the Device's Manufacturer are anonymised, and that the Panel shall remove or redact information where it considers that publishing such information would be prejudicial to the interests of one or more Parties, or pose a risk of Compromise to the DCC Total System, User Systems, RDP Systems and/or Devices.

H14.45 A decision of the Panel under Section H14.43 is merely intended to facilitate resolution of the relevant Testing Issue. A decision of the Panel under Section H14.43 is without prejudice to any future decision by the Change Board and/or the Authority concerning a Modification Proposal, by the Secretary of State in exercising its powers under section 88 of the Energy Act 2008, by the Authority concerning the DCC's compliance with the DCC Licence, or by the Panel under Section M8 (Suspension, Expulsion and Withdrawal).

Radio Frequency Noise Testing

H14.46 The DCC shall provide a Testing Service (referred to as RF Noise Testing) to enable Testing Participants to test Devices to ensure they meet the requirements of the current Intimate Communications Hub Interface Specification (ICHIS) published on the DCC Website in accordance with SEC Section H12, so they do not impact WAN or HAN performance.

H14.47 The following shall apply in respect of RF Noise Testing:

(a) the following persons shall be eligible to undertake RF Noise Testing: Parties and persons that have signed agreements based on the Specimen Enabling Services Agreement (subject only to such variations from such specimen form as are reasonable in the circumstances, including so as to require compliance with this Section H14);

(b) Testing Participants undertaking RF Noise Testing must each comply with such reasonable supplemental obligations as the DCC may notify to them from time to time (provided that such obligations are not inconsistent with the provisions of the Code that are in effect at that time); and

(c) the Testing Issue Resolution Process in Section H14.47 to H14.55 (General: Testing Issue Resolution Process) shall not apply to RF Noise Testing, but DCC must take reasonable steps to provide support and assistance to a person undertaking RF Noise Testing in order to assist that person in resolving Testing Issues encountered when undertaking RF Noise Testing.

H14.48 The DCC and the relevant Testing Participant in respect of the RF Noise Testing shall comply with any and all additional obligations concerning RF Noise Testing set out in the Enduring Testing Approach Document.

Interoperability and Innovation Events

H14.49 The DCC shall, from time to time and at its discretion, provide a Testing Service that provides a platform for Testing Participants to test connectivity, interoperability, interchangeability and functionality between SMETS2+ Devices.

H14.50 The DCC and the relevant Testing Participants in respect of Interoperability and Innovation Events shall comply with any and all additional obligations concerning Interoperability and Innovation Events set out in the Enduring Testing Approach Document.

GFI Testing

H14.51 The DCC shall provide GFI Testing Tools to Testing Participants upon request to support GFI Testing.

H14.52 The following shall apply in respect of GFI Testing:

(a) the following persons shall be eligible to undertake GFI Testing: Parties and persons that have signed agreements based on the Specimen Enabling Services Agreement (subject only to such variations from such specimen form as are reasonable in the circumstances, including so as to require compliance with this Section H14);

(b) the references in H14.42 to “Communications Hubs”, “DCC Systems” and “Devices” shall be interpreted as including references to prototypes of simulations of those things (and GFI Testing shall not include communication via the SM WAN, or a simulation of the SM WAN);

(c) Testing Participants undertaking GFI Testing must each comply with such reasonable supplemental obligations as the DCC may notify to them from time to time (provided that such obligations are not inconsistent with the provisions of the Code that are in effect at that time); and

(d) the Testing Issue Resolution Process in Section H14.47 to H14.55 (General: Testing Issue Resolution Process) shall not apply to GFI Testing, but DCC must take reasonable steps to provide support and assistance to a person undertaking GFI Testing in order to assist that person in resolving Testing Issues encountered when undertaking GFI Testing.

H14.53 The DCC and the relevant Testing Participant in respect of the GFI Testing shall comply with any and all additional obligations concerning GFI Testing set out in the Enduring Testing Approach Document.

Wired Instrumented Test Communications Hubs

H14.54 The DCC shall provide a Testing Service, which enables Testing Participants to undertake interoperability testing and message handling with a Test Communications Hub across a wired interface.

H14.55 The DCC and the relevant Testing Participant in respect of the Wired ITCH shall comply with any and all additional obligations concerning Wired ITCH set out in the Enduring Testing Approach Document.

DCC Boxed

H14.56 The DCC shall provide DCC Boxed to Testing Participants upon request, and subject to such Testing Participant agreeing to pay the applicable Charges.

H14.57 The following shall apply in respect of DCC Boxed:

(a) the following persons shall be eligible to use DCC Boxed: (i) Parties and (ii) persons that have signed agreements in accordance with Section H14.7;

(b) the Testing Issue Resolution Process in Section H14.37 to H14.45 (General: Testing Issue Resolution Process) shall not apply to DCC Boxed, but Section H14.33 shall apply in relation to DCC Boxed, so that the DCC must (subject to payment of the applicable Charges) take reasonable steps to provide support and assistance to a person using DCC Boxed in order to assist that person in resolving Testing Issues encountered when using DCC Boxed.

H14.58 The DCC and the relevant Testing Participant in respect of DCC Boxed shall comply with any and all additional obligations concerning DCC Boxed set out in the Enduring Testing Approach Document.

H15. DCC GATEWAY CONNECTIONS

Obligation to Maintain DCC Gateway Connections

H15.1 The DCC shall maintain each DCC Gateway Connection and make it available subject to and in accordance with the provisions of this Section H15.

H15.2 The DCC shall ensure that each DCC Gateway Connection is available at all times (subject to Planned Maintenance undertaken in accordance with Section H8.3).

H15.3 No Party may use a DCC Gateway Connection for any purposes other than accessing, and sending and receiving Data via, the DCC Interfaces (and subject to the provisions of this Code applicable to each DCC Interface).

Requests for DCC Gateway Connections

H15.4 Each Party other than the DCC may request (in accordance with this Section H15 and as further described in the DCC Gateway Code of Connection) as many DCC Gateway Connections as the Party wishes, in each case using the DCC Gateway Bandwidth Option of the Party's choice.

H15.5 In order to assist a Party in determining which DCC Gateway Bandwidth Option to request (or, in the case of connections using a DCC Gateway HV Connection, the size of the bandwidth required), the DCC shall (on request) provide any Party with information regarding the size of the different message types that can be sent via the DCC User Interface.

H15.6 Within 5 Working Days following receipt of any request from a Party for a DCC Gateway Connection at a premises, the DCC shall:

(a) where the request does not include all the information required in accordance with the DCC Gateway Connection Code of Connection, notify the Party that this is the case and provide reasonable assistance to the Party in re-submitting its request; or

(b) undertake a desk-based assessment as described in the DCC Gateway Connection Code of Connection, and provide a response to the Party in respect of that premises under Section H15.7, H15.8 or H15.9 (as applicable).

H15.7 In the case of a request for a DCC Gateway LV Connection, and where the DCC's desk-based assessment indicates that a physical site assessment is not required, the DCC shall provide an offer to the Party setting out:

(a) the DCC's reasonable estimate of the likely bandwidth of the connection once made;

(b) the date from which the DCC will provide the connection;

(c) the connection Charges and annual Charges that will apply in respect of the connection; and

(d) the connection period for which the connection will be made available.

H15.8 In the case of a request for a DCC Gateway LV Connection, and where the DCC's desk-based assessment indicates that a physical site assessment is required, the DCC shall notify the requesting Party that this is the case, and (unless the DCC is not reasonably able to do so without undertaking a physical site assessment, and subject to further information which may become available as a result of the physical site assessment) notify the Party of:

(a) the DCC's reasonable estimate of the likely bandwidth of the connection once made;

(b) the date from which the DCC will provide the connection;

(c) the connection Charges and annual Charges that will apply in respect of the connection; and

(d) the connection period for which the connection will be made available.

H15.9 In the case of a request for a DCC Gateway HV Connection, the DCC shall notify the Party that a physical site assessment is required, and (unless the DCC is not reasonably able to do so without undertaking a physical site assessment, and subject to further information which may become available as a result of the physical site assessment) notify the Party of:

(a) the date from which the DCC will provide the connection;

(b) the connection Charges and annual Charges that will apply in respect of the connection; and

(c) the connection period for which the connection will be made available.

Physical Site Assessments

H15.10 In the case of a notice to a Party under Section H15.8 or H15.9, the Party has 30 days following receipt of such notice to confirm to the DCC that the Party wishes the DCC to proceed with the physical site assessment. In the absence of such confirmation, the Party shall be deemed to have opted not to proceed.

H15.11 Where the DCC has received a confirmation in accordance with Section H15.10, then the DCC shall, within 30 days thereafter, complete the physical site assessment. The Party requesting the connection shall ensure that the DCC has such access to the Party's premises as the DCC may reasonably require in order to undertake such site assessment. The DCC shall ensure that all persons exercising such rights of access do so in compliance with the applicable site rules and reasonable instructions of those in control of the premises.

H15.12 The DCC shall, within 10 Working Days after completing a physical site assessment pursuant to Section H15.11, provide an offer to the Party that requested a connection at that premises setting out:

(a) any supplementary conditions which will apply in respect of the connection (in addition to the provisions of this Code) required as a consequence of matters identified in the site assessment;

(b) (in the case of DCC Gateway LV Connections) the DCC's reasonable estimate of the likely bandwidth of the connection once made;

(c) the date from which the DCC will provide the connection;

(d) the connection Charges and annual Charges that will apply in respect of the connection; and

(e) the connection period for which the connection will be made available.

Initial Provision of a DCC Gateway Connection

H15.13 In the case of an offer to a Party under Section H15.7 or H15.12, the Party has 30 days following receipt of such offer to confirm to the DCC that the Party accepts that offer. In the absence of such confirmation, the Party shall be deemed to have opted not to accept the offer (which shall lapse).

H15.14 Where a Party accepts an offer as described in Section H15.13, the DCC shall take all reasonable steps to provide the requested DCC Gateway LV Connection or DCC Gateway HV Connection by the date set out in the accepted offer (subject to payment of any applicable Charges).

H15.15 In the event that the DCC will be delayed in providing the requested DCC Gateway Connection, the DCC shall notify the relevant Party of the delay (including reasons for the delay) and of the revised connection date (being as soon a reasonably practicable thereafter), and shall take all reasonable steps to provide the requested connection by that revised date.

Use of a DCC Gateway Connection

H15.16 Subject to Section H15.3, the Party that requested a DCC Gateway Connection at a premises shall be entitled to use that connection for as long as the DCC is obliged to make it available in accordance with Section H15.18 (provided that such Party may transfer its right in respect of that DCC Gateway Connection to another Party on both such Parties giving notice to the DCC referring to this Section H15.16).

H15.17 The DCC Gateway Party may notify the DCC of the other Parties (if any) that are (subject to Section H15.3) entitled to share (or no longer entitled to share) use of that DCC Gateway Connection, and in respect of which DCC Interfaces.

Ongoing Provision of a DCC Gateway Connection

H15.18 Once a DCC Gateway Connection has been established at a premises on behalf of a DCC Gateway Party:

(a) the DCC shall make the connection available to the DCC Gateway Party in accordance with this Code until the DCC Gateway Party notifies the DCC that the Party wishes to cancel the connection (on not less than three months' prior notice);

(b) the DCC shall give the DCC Gateway Party four months' advance notice of the date on which the period of connection referred to in the accepted connection offer is due to expire (or of the date on which any period of extension pursuant to paragraph (c) below is due to expire), and shall at the same time confirm the annual Charges that will apply if the connection is not cancelled;

(c) on the expiry of a period referred to in paragraph (b) above, unless the DCC Gateway Party cancels the connection in accordance with paragraph (a) above, the period of connection shall be extended for a year (which will give rise to an additional annual Charge);

(d) the DCC Gateway Party and the DCC shall comply with the provisions of the DCC Gateway Connection Code of Connection applicable to the DCC Gateway Bandwidth Option utilised at the connection (and the DCC may limit the use of the connection where the DCC Gateway Party fails to do so and where this is provided for in the DCC Gateway Connection Code of Connection);

(e) the DCC shall, on request, provide the DCC Gateway Party with a report on the performance of its connection as further set out in the DCC Gateway Connection Code of Connection; and

(f) in the case of DCC Gateway HV Connections, the DCC Gateway Party may increase or decrease the bandwidth of its connection in accordance with (and subject to the limitation provided in) the DCC Gateway Code of Connection (provided that, in the case of decreases, the applicable Charges may not alter as a result).

H15.19 The cancellation of any DCC Gateway Connection pursuant to Section H15.18(a), is without prejudice to:

(a) the right of the DCC Gateway Party to apply for another connection under Section H15.4; and

(b) the obligation of the DCC Gateway Party to pay the applicable Charges for the full duration of the period of connection referred to in the accepted connection offer or any period of extension under Section H15.18(c).

DCC Gateway Equipment

H15.20 In first providing a DCC Gateway Connection at a premises, the DCC shall procure that the DCC Gateway Equipment is installed at the relevant premises, and that the DCC Gateway Equipment is installed in accordance with Good Industry Practice and all applicable Laws and Directives.

H15.21 Following its installation at a premises, the DCC shall ensure that the DCC Gateway Equipment is operated and maintained in accordance with Good Industry Practice, and that it complies with all applicable Laws and Directives. The DCC shall maintain a record of the DCC Gateway Equipment installed at each DCC Gateway Party's premises from time to time, and of the point of its connection to that Party's Systems.

H15.22 The DCC Gateway Party at whose premises the DCC Gateway Equipment is (or is to be) installed shall provide the DCC with such access to that premises as the DCC may reasonably require in order to allow it to undertake the installation, maintenance, relocation or removal of the DCC Gateway Equipment. The DCC shall ensure that all persons exercising such rights of access do so in compliance with the site rules and reasonable instructions of the DCC Gateway Party.

H15.23 The DCC Gateway Party at whose premises the DCC Gateway Equipment is (or is to be) installed shall be entitled to witness and inspect the installation, maintenance, relocation or removal of the DCC Gateway Equipment. No such witnessing or assessment shall relieve the DCC of its obligations under this Code.

H15.24 Each DCC Gateway Party shall ensure that no damage is deliberately or negligently caused to the DCC Gateway Equipment installed at its premises (save that such a Party may take emergency action in accordance with Good Industry Practice to protect the health and safety of persons or to prevent imminent damage to property).

H15.25 The DCC Gateway Equipment shall (as between the DCC and each other Party) remain the property of the DCC. The DCC Gateway Equipment is installed at the DCC's risk, and no other Party shall have liability for any loss of or damage to the DCC Gateway Equipment unless and to the extent that such loss or damage arose as a result of that Party's breach of this Code (including that Party's obligations under Section H15.24).

H15.26 No Party other than the DCC shall hold itself out as the owner of the DCC Gateway Equipment, or purport to sell or otherwise dispose of the DCC Gateway Equipment.

H15.27 Where a DCC Gateway Party wishes to alter the location of the DCC Gateway Equipment at the Party's premises, then that Party shall make a request to the DCC, and the DCC shall either (in accordance with any provisions of the DCC Gateway Connection Code of Connection concerning the same):

(a) notify such Party that it is entitled to relocate the DCC Gateway Equipment within the Party's premises, in which case the Party may move such equipment (and, where it does so, it shall do so in accordance with Good Industry Practice and all applicable Laws and Directives); or

(b) notify such Party that the DCC Gateway Equipment must be relocated by the DCC, in which case the DCC shall (subject to payment of any applicable Charges) move the DCC Gateway Equipment in accordance with Good Industry Practice and all applicable Laws and Directives.

H15.28 Where the DCC's obligation to make a DCC Gateway Connection available ends in accordance with Section H15.18(a) or the DCC Gateway Party for a DCC Gateway Connection ceases to be a Party in accordance with Section M8 (Suspension, Expulsion and Withdrawal), then the DCC shall, within 30 days thereafter:

(a) cease to make that DCC Gateway Connection available; and

(b) remove the DCC Gateway Equipment from the relevant premises in accordance with Good Industry Practice and all applicable Laws and Directives.

DCC Gateway Connection Disputes

H15.29 Where a DCC Gateway Party wishes to raise a dispute in relation to its request for a DCC Gateway Connection (or the extension of its period of connection or increases or decreases in the bandwidth of its connection, in each case under Section H15.18), then the dispute may be referred to the Panel for determination. Where that Party or the DCC disagrees with any such determination, then it may refer the matter to the Authority for its determination, which shall be final and binding for the purposes of this Code.

H16. INTEROPERABILITY CHECKER SERVICE

The Responsibility of Supplier Parties

H16.1 Each Supplier Party shall ensure that Energy Consumers at premises supplied by it with electricity and/or gas shall:

(a) have access to the information described in Section H16.2;

(b) be able to access that information in the manner described in Section H16.4; and

(c) have such access in such manner during the period determined in accordance with Section H16.5.

H16.2 The information described in this Section (the "**Interoperability Data**") is, in respect of each premises, information as to:

(a) whether the supply of electricity or the supply of gas (as determined by the request made by the Energy Consumer) to the premises is made through an Enrolled Smart Metering System; and

(b) where either the supply of electricity or the supply of gas is made through an enrolled Smart Metering System:

(i) whether the supply of other fuel is also made through an Enrolled Smart Metering System;

(ii) the name of the Electricity Supplier or the name of the Gas Supplier (or both as the case may be);

(iii) whether any such Enrolled Smart Metering System is a SMETS1 Smart Metering System or a SMETS2+ Smart Metering System; and

(iv) where any such Enrolled Smart Metering System is a SMETS1 Smart Metering System, the name of each electricity and/or gas supplier (as the case may be) which has notified the DCC that it is its policy, if it commences to supply premises at which a Smart Metering System of that type is installed, to operate that Smart Metering System in Smart Mode.

H16.3 For the purposes of Section H16.2(b)(iv), the name of the electricity or gas supplier shall include, where applicable, any brand name that the electricity or gas supplier has notified to the DCC as a brand name that it uses in any communications with or to Energy Consumers.

H16.4 The Interoperability Data in respect of any premises shall be able to be accessed by each Energy Consumer at those premises on the request of that Energy Consumer, by means of remote communications, and free of charge.

H16.5 The Interoperability Data shall be capable of being accessed by an Energy Consumer:

(a) from any such date as may be specified in a direction issued by the Secretary of State to all Supplier Parties and the DCC; and

(b) until any such date as may be specified in a further direction issued by the Secretary of State to all Supplier Parties and the DCC,

and for these purposes the Secretary of State may exercise the power to give a direction under Sections H16.5(a) and (b) more than once.

Provision of Data by Suppliers to the DCC

H16.6 For the purpose of establishing a record of the Interoperability Data referred to in Section H.16.2(b)(iv), each Supplier Party may provide the DCC, in such manner and in such form as may be specified by the DCC, with a statement which:

(a) is in respect of each type of Smart Metering System which at that time constitutes an Enrolled SMETS1 Smart Metering System at any premises;

(b) indicates whether the policy of that Supplier Party, if it commenced (at the date of the statement) to supply premises at which that type of Smart Metering System was installed, would be, subject to any exceptions identified by the Licensee in the statement, to operate it in Smart Mode; and

(c) is accurate and up to date.

H16.7 Where a Supplier Party provides a statement to the DCC in accordance with Section H16.6, it may also notify the DCC of any brand name (including where it works in partnership with a White Label Tariff Provider any brand name of the White Label Tariff Provider) it uses when engaging in activities that are directed at, or incidental to identifying and communicating with, Energy Consumers in relation to the supply of electricity or gas.

Obligations of the DCC

H16.8 On behalf of all Supplier Parties, and for the purpose of ensuring that each Supplier Party can discharge its responsibility under Section H16.1, the DCC shall provide a service to be known as the " **Interoperability Checker Service**", being a service:

(a) by means of which the Interoperability Data in respect of each premises to which gas and/or electricity is supplied shall be made available to Energy Consumers at those premises so that it may be accessed by each Energy Consumer on request and free of charge by means of remote communications; and

(b) that is provided during the period determined in accordance with Section H16.5.

H16.9 For the purpose of providing the Interoperability Checker Service in accordance with Section H16.8, the DCC shall enter into an agreement in accordance with Sections H16.10 to H16.12 with either:

(a) Citizens Advice and Citizens Advice Scotland; or

(b) such other person as may, in substitution for those named in paragraph (a), be specified in a direction issued by the Secretary of State to the DCC.

H16.10 The agreement referred to in Section H16.9 shall be an agreement under which the person identified in that Section shall, by means of:

(a) one or more dedicated pages on a website; or

(b) a dedicated smartphone or tablet application,

maintained by it or on its behalf, agree to provide a facility through which Energy Consumers may request and obtain the Interoperability Data via remote communications.

H16.11 The agreement referred to in Section H16.9 shall, as a minimum, contain terms which require that the facility provided under that agreement is designed to ensure that:

(a) any person requesting Interoperability Data shall be able to obtain the such data only on providing information that reasonably establishes that he or she is an Energy Consumer at the premises to which the Interoperability Data relates;

(b) appropriate safeguards are in place to ensure that Interoperability Data may be accessed only by individual Energy Consumers, and may not be accessed by means of software capable of making automated requests in respect of multiple premises;

(c) no Interoperability Data, or any information provided by Energy Consumers for the purposes of requesting the Interoperability Data, may be accessed, retained or processed by the person providing the facility:

(i) in such a manner as may be used to provide, or used in conjunction with the provision of, any other service by that person to an Energy Consumer; or

(ii) for any purpose other than ensuring the effective provision of the facility.

H16.12 A copy of the agreement entered into by the DCC in accordance with Section H16.9 shall, as soon as practicable after it has been entered into, be submitted by the DCC to the Secretary of State.

H16.13 The DCC shall have no liability to any Party where it provides (or does not provide) the Interoperability Checker Service in circumstances where it should not (or should) have done so, to the extent that the same arises due to inaccuracies in the Interoperability Data that are not caused by the DCC.

Provision of Data by the DCC to Suppliers

H16.14 The DCC shall provide Supplier Parties, in such manner and in such form as may be determined from time to time by the DCC, with a statement that sets out each particular type of SMETS1 Smart Metering System which at that time is or can become an Enrolled SMETS1 Smart Metering System.

Definitions

H16.15 For the purposes of this Section H16:

Smart Mode	means, in respect of a Smart Metering System of a particular type, that a Supplier Party does or will, on a regular basis, send communications to and receive communications from that Smart Metering System by means of the DCC's Communications Services.

H17. MAP / MANUFACTURER REPORTS

H17.1 Subject to Section H17.2, the following entities shall be eligible to request and receive reports under this Section H17 in respect of Smart Meters: (a) the Manufacturer of the Smart Meter; and/or (b) the Meter Asset Provider of the Smart Meter.

H17.2 The DCC shall only provide reports under this Section H17 to Meter Asset Providers and Manufacturers which are either: (a) a Party; or (b) party to an agreement in the form of the Specimen Enabling Services Agreement.

H17.3 In order to receive reports in respect of a particular Smart Meter, the entity requesting the report will need to provide reasonable evidence to the DCC that such entity is the Manufacturer or Meter Asset Provider of the Smart Meter. The DCC shall not provide reports to an entity unless the DCC has obtained such reasonable evidence of such entity's status as Manufacturer or Meter Asset Provider.

H17.4 Reports under this Section H17 can be requested quarterly, monthly or on an ad hoc basis (but not more than once each month). The DCC shall provide the reports in accordance with such requests.

H17.5 Each report under this Section H17 will set out for each and every Smart Meter for which the recipient is the Manufacturer or Meter Asset Provider:

(a) Smart Meter ID;

(b) Smart Meter Type, Smart Meter Model and Manufacturer;

(c) firmware version;

(d) SMI Status;

(e) Region;

(f) the Registered Supplier(s) and its/their effective from date(s); and

(g) Communications Hub make, model and firmware version.

H17.6 The DCC shall provide reports under this Section H17 via its preferred file sharing platform, and shall mark them as confidential and not to be shared with any third party apart from the Registered Supplier Party.

H17.7 Each entity which obtains one or more reports pursuant to this Section H17 undertakes to:

(a) only use the data contained in those reports for its internal business purposes;

(b) not sell or commercially exploit the data contained in those reports; and

(c) keep the data contained in those reports confidential in accordance with Section M4 (Confidentiality).

Contents

I DATA PRIVACY

I1. DATA PROTECTION AND ACCESS TO DATA

Without Prejudice

I1.1 The obligations of the DCC and each User under this Section I1 are without prejudice to any other obligations they each may have under the Data Protection Legislation and other Relevant Instruments, including any such obligations they each may have concerning Processing of Personal Data.

User Obligations

Consumption Data

I1.2 Each User undertakes that it will not request, in respect of a Smart Metering System, a Communication Service or Local Command Service that will result in it obtaining Consumption Data, unless:

(a) the User has the Appropriate Permission in respect of that Smart Metering System; and

(b) (where that User is not the Import Supplier, Export Supplier, Gas Supplier, Electricity Distributor or Gas Transporter for that Smart Metering System) the User has, at the point of obtaining Appropriate Permission and at such intervals as are reasonably determined appropriate by the User for the purposes of ensuring that the Energy Consumer is regularly updated of such matters, notified the Energy Consumer in writing of:

(i) the time periods (by reference to length) in respect of which the User obtains or may obtain Consumption Data;

(ii) the purposes for which that Consumption Data is, or may be, used by the User; and

(iii) the Energy Consumer’s right to object or withdraw consent (as the case may be) to the User obtaining or using that Consumption Data, and the process by which the Energy Consumer may object or withdraw consent.

Service Requests

I1.3 Each User undertakes that it will not send either a 'Join Service' or 'Unjoin Service' Service Request (respectively to join a Type 2 Device to, or unjoin it from, any Smart Meter or Device Associated with a Smart Meter) unless:

(a) the User is the Responsible Supplier for the Smart Meter or Associated Device to which the Service Request is sent, and sends that Service Request for the purpose of complying with an obligation under its Energy Supply Licence; or

(b) the Energy Consumer at the premises at which the Smart Meter is located has given the User Unambiguous Consent, which has not been withdrawn, to (as the case may be):

(i) join that Type 2 Device to the Smart Meter or Associated Device, and the User has clearly informed the Energy Consumer before obtaining such Unambiguous Consent that a consequence of joining the Type 2 Device may be that Data relating to the Energy Consumer will be shared with third parties; or

(ii) unjoin it from the Smart Meter or Associated Device, save that the Responsible Supplier for a Smart Metering System at the premises need not obtain such Unambiguous Consent where it has reasonable grounds to believe that the Type 2 Device has Compromised or is likely to Compromise any Device forming part of that Smart Metering System (and the Responsible Supplier shall, where it unjoins a Type 2 Device in such circumstances, take all reasonable steps to inform the Energy Consumer that it has done so).

Access to Records

I1.4 Each User undertakes that it will not access (pursuant to Section H8.16) or request (pursuant to Section H8.17) the information described in Section H8.16(c), unless:

(a) the Energy Consumer at the premises at which the relevant Smart Meter is located has given the User Unambiguous Consent to do so and such consent has not been withdrawn; and

(b) the information is accessed solely for the purpose of its provision to that Energy Consumer.

Good Industry Practice

I1.5 Each User shall put in place and maintain arrangements designed in accordance with Good Industry Practice to ensure that each person from whom it has obtained consent pursuant to Section I1.2 to I1.4 is the Energy Consumer.

Processing of Personal Data by the DCC

I1.6 It is acknowledged that, in providing the Services to a User, the DCC may act in the capacity of 'Data Processor' on behalf of that User in respect of the Personal Data for which that User is the 'Data Controller'.

I1.6A The Personal Data which the DCC will Process as a Data Processor on behalf of Users will relate to Energy Consumers, and will include Personal Data which is included within messages sent and received by the DCC via the DCC User Interface or the Self- Service Interface, and/or which is included within messages sent or received by the DCC to or from Communications Hubs. The nature of such Personal Data will be that which is required or permitted to be included in such messages as described in this Code. The full description of the subject matter, the nature and purpose of the processing, and the type of personal data is as described by this Code as a whole.

I1.7 The DCC undertakes for the benefit of each User in respect of the Personal Data for which that User is the 'Data Controller' to:

(a) only Process that Personal Data for the purposes permitted by the DCC Licence and this Code (subject to paragraph (d) below);

(b) only Process that Personal Data for so long as it is required to do so by the DCC Licence and this Code;

(c) undertake the Processing of that Personal Data in accordance with the DCC Licence and this Code, (to the extent consistent with the DCC Licence and this Code) on the documented instructions of the User, and (subject to the foregoing requirements of this Section I1.7(c)) not in a manner that the DCC knows (or should reasonably know) is likely to cause the User to breach its obligations under the Data Protection Legislation (subject to paragraph (d) below);

(d) if the DCC is aware that, or is of the opinion that, any requirement of paragraph (a) (b) or (c) above infringes the Data Protection Legislation, the DCC shall immediately inform the User of this giving details of the infringement or potential infringement (unless the DCC is prohibited from doing so by any of its other obligations under Laws and Directives);

(e) ensure that the DCC's personnel who are authorised to Process Personal Data are under enforceable obligations of confidentiality and are required only to Process that Personal Data in accordance with the DCC's obligations under the DCC Licence and this Code;

(f) having regard to the state of the art, the costs of implementation and the nature, scope, context and purposes of Processing as well as the risk of varying likelihood and severity for the rights and freedoms of Data Subjects, implement appropriate technical and organisational measures to protect that Personal Data in particular from accidental or unlawful loss, destruction, alteration or unauthorised disclosure of, or access to personal data transmitted, stored or otherwise Processed (such measures to at least be in accordance with Good Industry Practice and the requirements of Section G (Security));

(g) taking into account the nature of the Processing assist the User with its obligations to comply with Data Subjects' requests and Data Subjects' rights under the Data Protection Legislation in respect of that Personal Data through, insofar as is possible, the use of appropriate technical and organisational measures;

(h) taking into account the nature of the Processing and the information available to the DCC, assist the User in ensuring compliance with the User's obligations in Articles 32-36 of the General Data Protection Regulation (or its national equivalent), including:

  (i) notifying the User without undue delay if the DCC becomes aware of a breach of the Data Protection Legislation in relation to the Personal Data (including in the event of unauthorised access to such Personal Data); and

  (ii) providing full details of the relevant breach where caused by the DCC or any Sub-Processor without undue delay or, where necessary, in phases but always without further undue delay;

(i) provide reasonable assistance to the User in complying with any enquiry made, or investigation or assessment initiated, by the Information Commissioner or any other Competent Authority in respect of the Processing of that Personal Data pursuant to this Code;

(j) promptly notify the User in the event that the DCC Processes any of that Personal Data otherwise than in accordance with this Code (including in the event of unauthorised access to such Personal Data);

(k) notify the User of any complaint relating to the DCC's obligations under the Data Protection Legislation in respect of the Processing of that Personal Data pursuant to this Code;

(l) after the end of the provision of the Services to which the Processing of that Personal Data relates, at the written election of the User, either securely destroy the Personal Data or return it to the User together with all copies (save to the extent that the DCC is required by Laws and Directives to retain a copy of the Personal Data) and permit the Independent Privacy Auditor (on the instruction of SECCo on behalf of Users collectively), on giving reasonable prior notice of its intention to audit,

(m) to audit the DCC's compliance with this Section I1.7 during normal business hours, and shall make available to the Independent Privacy Auditor all information, systems and staff reasonably necessary for the Independent Privacy Auditor to conduct such audit. The number of audits shall be limited to no more than once in every twelve (12) calendar month period unless more frequent audits are required under the Data Protection Legislation or the Panel has grounds to suspect there has or is likely to be a breach of the Data Protection Legislation. Where practicable, DCC shall be provided with an opportunity to comment upon the scope of an audit in advance and any audit shall be carried out in such a way that interruption to DCC's operations is minimised as far as is reasonably possible.

DCC's Sub-Processors

I1.8 The DCC shall ensure that its Sub-Processor(s) are subject to written contractual obligations in respect of the Processing of Personal Data which are at least equivalent to the obligations imposed on the DCC under the DCC Licence and this Code, including obligations which provide sufficient guarantees from the Sub-Processor that the Processing meets the requirements stated at any time in the Data Protection Legislation.

I1.9 Each User hereby gives its general authorisation to the DCC to engage Sub-Processor(s) who are appointed in accordance with the DCC Licence and does not object to the engagement by the DCC of any Sub-Processor provided that in engaging the Sub- Processor the DCC complies with the DCC Licence and this Code and publishes on its Website the identity of the Sub-Processor(s) from time to time. Each User hereby consents to Processing by each such Sub-Processor who is appointed in accordance with the DCC Licence and this Code.

Records

I1.10 The DCC and each User will each maintain in accordance with Good Industry Practice all such records and other information as is necessary to enable the DCC and each such User to demonstrate that it is complying with its respective obligations under Sections I1.2 to I1.9.

I1.11 The DCC shall make available to each User all information reasonably necessary to demonstrate compliance by the DCC with Sections I1.6 to I1.9, but only insofar as such information relates to the Personal Data for which that User is the Data Controller.

General Compliance with Data Protection Legislation

I1.12 Each of the DCC, SECCo, and each User undertakes to comply with its obligations under the Data Protection Legislation in respect of Personal Data they Process as a Data Controller or Data Processor pursuant to this Code.

Permission for Gas Supplier to Store Data on Shared SMETS1 Installation

I1.13 In the case of a SMETS1 GSME which forms part of the same SMETS1 Installation as a SMETS1 ESME, and where the Gas Supplier for the SMETS1 GSME is a different person to the Import Supplier for the SMETS1 ESME, the Import Supplier hereby agrees to permit the Gas Supplier to store Data on the SMETS1 GPF which forms part of that SMETS1 Installation in the manner envisioned by SMETS1.

I2. OTHER USER PRIVACY AUDITS

Procurement of the Independent Privacy Auditor

I2.1 The Panel shall procure the provision of privacy audit services:

(a) of the scope specified in Section I2.3;

(b) from a person who:

(i) is suitably qualified, and has the necessary experience and expertise, to provide those services; and

(ii) is suitably independent in accordance with Section I2.4,

and that person is referred to in this Section I2 as the "**Independent Privacy Auditor**".

I2.2 The Panel may appoint more than one person to carry out the functions of the Independent Privacy Auditor.

Scope of Privacy Audit Services

I2.3 The privacy audit services specified in this Section I2.3 are services in accordance with which, for the purpose of providing reasonable assurance that Other Users are complying with their obligations under Sections I1.2 to I1.5 (User Obligations), the Independent Privacy Auditor shall:

(a) carry out Privacy Assessments at such times and in such manner as is provided for in this Section I2;

(b) produce Privacy Assessment Reports in relation to Other Users that have been the subject of a Privacy Assessment;

(c) receive and consider Privacy Assessment Responses;

(d) otherwise, at the request of, and to an extent determined by, the Panel carry out an assessment of the compliance of any Other User with its obligations under Sections I1.2 to I1.5;

(e) provide to the Panel such advice and support as may be requested by it from time to time, including in particular advice in relation to the suitability of any remedial action plan for the purposes of Section M8.4 of the Code (Consequences of an Event of Default);

(f) provide to the Authority such advice and support as it may request in relation to any disagreements with a decision of the Panel in respect of which the Authority is required to make a determination in accordance with this Section I2; and

(g) undertake such other activities, and do so at such times and in such manner, as may be further provided for in this Section I2.

Independence Requirement

I2.4 The Independent Privacy Auditor shall be treated as suitably independent in accordance with this Section I2.4 only if it satisfies:

(a) the requirements specified in Section I2.6; and

(b) the requirement specified in Section I2.7.

I2.5 For the purposes of Sections I2.6 and I2.7:

(a) a "**Relevant Party**" means any Party in respect of which the Independent Privacy Auditor carries out functions under this Section I2; and

(b) a "**Relevant Service Provider**" means any service provider to a Relevant Party from which that Party acquires capability for a purpose related to its compliance with its obligations as an Other User under Section I1.2 to I1.5.

I2.6 The requirements specified in this Section I2.6 are that:

(a) no Relevant Party or any of its subsidiaries, and no Relevant Service Provider or any of its subsidiaries, holds or acquires any investment by way of shares, securities or other financial rights or interests in the Independent Privacy Auditor;

(b) no director of any Relevant Party, and no director of any Relevant Service Provider, is or becomes a director or employee of, or holds or acquires any investment by way of shares, securities or other financial rights or interests in, the Independent Privacy Auditor; and

(c) the Independent Privacy Auditor does not hold or acquire a participating interest (as defined in section 421A of the Financial Services and Markets Act 2000) in any Relevant Party or any Relevant Service Provider,

(but for these purposes references to a Relevant Service Provider shall not include the Independent Privacy Auditor where it acts in that capacity).

I2.7 The requirement specified in this Section I2.7 is that the Independent Privacy Auditor is able to demonstrate to the satisfaction of the Panel that it has in place arrangements to ensure that it will at all times act independently of any commercial relationship that it has, has had, or may in future have with a Relevant Party or Relevant Service Provider (and for these purposes a 'commercial relationship' shall include a relationship established by virtue of the Independent Privacy Auditor itself being a Relevant Service Provider to any Relevant Party).

Compliance of the Independent Privacy Auditor

I2.8 The Panel shall be responsible for ensuring that the Independent Privacy Auditor carries out its functions in accordance with the provisions of this Section I2.

Other Users: Duty to Cooperate in Assessment

I2.9 Each Other User shall do all such things as may be reasonably requested by the Panel, or by any person acting on behalf of or at the request of the Panel (including in particular the Independent Privacy Auditor), for the purposes of facilitating an assessment of that Other User's compliance with its obligations under Sections I1.2 to I1.5.

I2.10 For the purposes of Section I2.9, an Other User shall provide the Panel (or the relevant person acting on its behalf or at its request) with:

(a) all such Data as may reasonably be requested, within such times and in such format as may reasonably be specified;

(b) all such other forms of cooperation as may reasonably be requested, including in particular:

(i) access at all reasonable times to such parts of the premises of that Other User as are used for, and such persons engaged by that Other User as carry out or are authorised to carry out, any activities related to its compliance with its obligations under Sections I1.2 to I1.5; and

(ii) such cooperation as may reasonably by requested by the Independent Privacy Auditor for the purposes of carrying out any Privacy Assessment in accordance with this Section I2.

Categories of Assessment

I2.11 I2.11 For the purposes of this Section I2, there shall be the following three categories of privacy assessment:

(a) a Full Privacy Assessment (as further described in Section I2.12);

(b) a Random Sample Privacy Assessment (as further described in Section I2.13); and

(c) a Privacy Self-Assessment (as further described in Section I2.14).

I2.12 A "**Full Privacy Assessment**" shall be an assessment carried out by the Independent Privacy Auditor in respect of an Other User to identify the extent to which that Other User:

(a) is compliant with each of its obligations under Sections I1.2 to I1.5; and

(b) has in place the systems and processes necessary for ensuring that it complies with each such obligation.

I2.13 A "**Random Sample Privacy Assessment**" shall be an assessment carried out by the Independent Privacy Auditor in respect of an Other User to identify the extent to which the Other User is compliant with each of its obligations under Sections I1.2 to I1.5 in relation to a limited (sample) number of Energy Consumers.

I2.14 A " **Privacy Self-Assessment**" shall be an assessment carried out by an Other User to identify the extent to which, since the last occasion on which a Privacy Assessment was carried out in respect of that Other User by the Independent Privacy Auditor, there has been any material change:

(a) in the arrangements that the Other User has in place to comply with its obligations under Sections I1.2 to I1.5; or

(b) in the quantity of Consumption Data being obtained by the Other User.

The Privacy Controls Framework

I2.15 The Panel shall develop and maintain a document to be known as the "**Privacy Controls Framework**" which shall:

(a) set out arrangements designed to ensure that Privacy Assessments are carried out appropriately for the purpose of providing reasonable assurance that Other Users are complying with (or, for the purposes of Section H1.10(d) (User Entry Process Requirements), are capable of complying with) their obligations under Sections I1.2 to I1.5; and

(b) for that purpose, in particular, specify the principles and criteria to be applied in the carrying out of any Privacy Assessment, including principles designed to ensure that Privacy Assessments take place on a consistent basis across all Other Users; and

(c) make provision for determining the timing, frequency and selection of Other Users for the purposes of Random Sample Privacy Assessments.

I2.16 In developing the Privacy Controls Framework, and prior to making any subsequent change to it, the Panel shall consult with and have regard to the views of all Parties, Citizens Advice and Citizens Advice Scotland, and the Authority.

I2.17 The Panel shall ensure that an up to date copy of the Privacy Controls Framework is made available to all Parties and is published on the Website.

Privacy Assessments: General Procedure

Privacy Controls Framework

I2.18 Each Privacy Assessment carried out by the Independent Privacy Auditor or an Other User shall be carried out in accordance with the Privacy Controls Framework.

The Privacy Assessment Report

I2.19 Following the completion of a Full Privacy Assessment or Random Sample Privacy Assessment, the Independent Privacy Auditor shall, in discussion with the Other User to which the assessment relates, produce a written report (a "**Privacy Assessment Report**") which shall:

(a) set out the findings of the Independent Privacy Auditor on all the matters within the scope of the Privacy Assessment;

(b) specify any instances of actual or potential non-compliance of the Other User with its obligations under Sections I1.2 to I1.5 which have been identified by the Independent Privacy Auditor;

(c) set out the evidence which, in the opinion of the Independent Privacy Auditor, establishes each of the instances of actual or potential non-compliance which it has identified.

I2.20 The Independent Privacy Auditor shall submit a copy of each Privacy Assessment Report to the Panel and to the Other User to which that report relates.

The Privacy Assessment Response

I2.21 Following the receipt by any Other User of a Privacy Assessment Report which relates to it, the Other User shall as soon as reasonably practicable, and in any event by no later than such date as the Panel may specify:

(a) produce a written response to that report (a "**Privacy Assessment Response**") which addresses the findings set out in the report; and

(b) submit a copy of that response to the Panel and the Independent Privacy Auditor.

I2.22 Where a Privacy Assessment Report specifies any instance of actual or potential non- compliance of an Other User with its obligations under Sections I1.2 to I1.5, the Other User shall ensure that its Privacy Assessment Response includes the matters referred to in Section I2.23.

I2.23 The matters referred to in this Section are that the Privacy Assessment Response:

(a) indicates whether the Other User accepts the relevant findings of the Independent Privacy Auditor and provides an explanation of the actual or potential non-compliance that has been identified; and

(b) sets out any steps that the Other User proposes to take in order to remedy and/or mitigate the actual or potential non-compliance, and identifies a timetable within which the Other User proposes to take those steps.

I2.24 Where a Privacy Assessment Response sets out any steps that an Other User proposes to take in accordance with Section I2.23(b), the Panel (having considered the advice of the Independent Privacy Auditor) shall review that response and either:

(a) notify the Other User that it accepts that the steps that the Other User proposes to take, and the timetable within which it proposes to take them, are appropriate to remedy and/or mitigate the actual or potential non-compliance specified in the Privacy Assessment Report; or

(b) seek to agree with the Other User such alternative steps and/or timetable as would, in the opinion of the Panel, be more appropriate for that purpose.

I2.25 Where a Privacy Assessment Response sets out any steps that an Other User proposes to take in accordance with Section I2.23(b), and where those steps and the timetable within which it proposes to take them are accepted by the Panel, or alternative steps and/or an alternative timetable are agreed between it and the Other User in accordance with Section I2.24, the Other User shall:

(a) take the steps that have been accepted or agreed (as the case may be) within the timetable that has been accepted or agreed (as the case may be); and

(b) report to the Panel:

(i) on its progress in taking those steps, at any such intervals or by any such dates as the Panel may specify;

(ii) on the completion of those steps in accordance with the timetable; and

(iii) on any failure to complete any of those steps in accordance with the timetable, specifying the reasons for that failure.

The Privacy Self-Assessment Report

I2.26 Following the completion of a Privacy Self-Assessment, the Other User which carried out that self-assessment shall as soon as reasonably practicable produce a written report (a "**Privacy Self-Assessment Report**") which shall set out the findings of the Other User, and describe the nature of any material change, since the last occasion on which a Privacy Assessment was carried out in respect of the Other User by the Independent Privacy Auditor, in respect of:

(a) the arrangements that the Other User has in place to comply with its obligations under Sections I1.2 to I1.5; or

(b) the quantity of Consumption Data being obtained by the Other User.

I2.27 A Other User which produced a Privacy Self-Assessment Report shall:

(a) ensure that the report is accurate, complete and not misleading; and

(b) submit a copy of the report to the Panel and the Independent Privacy Auditor.

I2.28 Within the period of time specified in the Privacy Controls Framework following the receipt by it of a Privacy Self-Assessment Report, the Independent Privacy Auditor shall either:

(a) notify the Other User that it accepts that report; or

(b) inform the Other User that it will be subject to an additional Privacy Assessment of such nature by such date as the Panel may specify.

Initial Full Privacy Assessment: User Entry Process

I2.29 Sections I2.31 to I2.36 set out the applicable privacy requirements referred to in Section H1.10(d) (User Entry Process Requirements).

I2.30 For the purposes of Sections I2.31 to I2.36, any reference in Sections I1.2 to I1.5 or the preceding provisions of this Section I2 to a 'User' or 'Other User' (or to any related expression which applies to Users), shall be read as including a reference (or otherwise applying) to any Party seeking to become a User by completing the User Entry Process for the User Role of Other User.

Initial Full Privacy Assessment

I2.31 For the purpose of completing the User Entry Process for the User Role of Other User, a Party wishing to act in that User Role shall be subject to a Full Privacy Assessment.

Panel: Setting the Assurance Status

I2.32 Following the receipt by it of the Privacy Assessment Report and Privacy Assessment Response produced after the initial Full Privacy Assessment, the Panel shall promptly consider both documents and set the assurance status of the Party, in relation to its compliance with each of its obligations under Sections I1.2 to I1.5, in accordance with Section I2.33.

I2.33 The Panel shall set the assurance status of the Party as one of the following:

(a) approved;

(b) approved, subject to the Party:

(i) taking such steps as it proposes to take in its Privacy Assessment Response in accordance with Section I2.23(b); or

(ii) both taking such steps and being subject to a further Privacy Assessment of such nature and by such date as the Panel may specify;

(c) deferred and:

(i) the Party having first taken such steps as it proposes to take in its Privacy Assessment Response in accordance with Section I2.23(b) and been subject to a further Privacy Assessment; and

(ii) the Panel having determined that it is satisfied, on the evidence of the further Privacy Assessment, that such steps have been taken; or

(d) rejected and:

(i) the Party shall have a second Full Privacy Assessment to address any issues identified by the Panel as being, in the opinion of the Panel, not adequately addressed in that response as submitted to Panel; and

(ii) upon completion of the second Full Privacy Assessment the Panel will reconsider the assurance status in accordance with Section I2.32.

Approval

I2.34 For the purposes of Sections H1.10(d) and H1.11 (User Entry Process Requirements):

(a) a Party shall be considered to have successfully demonstrated that it meets the applicable privacy requirements of this Section I2 when:

(i) the Panel has set its assurance status to 'approved' in accordance with either Section I2.33(a) or (b); or

(ii) the Panel has set its assurance status to 'deferred' in accordance with Section I2.33(c) and the requirements specified in that Section have been met; and

(b) the Panel shall notify the Code Administrator as soon as reasonably practicable after the completion of either event described in paragraph (a)(i) or (ii).

Obligations on an Approved Party

I2.35 Where the Panel has set the assurance status of a Party to 'approved subject to' specified in Section I2.33(b), the Party shall take the steps to which that approval is subject in accordance with that section.

Disagreement with Panel Decisions

I2.36 Where a Party disagrees with any decision made by the Panel in relation to it under Section I2.33, it may appeal that decision to the Authority and the determination of the Authority shall be final and binding for the purposes of the Code.

Privacy Assessments: Post-User Entry Process

I2.37 Following its initial Full Privacy Assessment for the purposes of the User Entry Process, an Other User shall be subject to annual Privacy Assessments as follows:

(a) in the first year after the year of its initial Full Privacy Assessment, to a Privacy Self-Assessment;

(b) in the immediately following year, to a Privacy Self-Assessment;

(c) in the next following year, to a Full Privacy Assessment; and

(d) in each year thereafter, to a category of Privacy Assessment which repeats the same annual sequence as that of paragraphs (a) to (c),

but these requirements shall be subject to the provisions of Section I2.38.

I2.38 An Other User:

(a) may, on the instruction of the Panel, or otherwise in accordance with the provisions of the Privacy Controls Framework, be subject to a Full Privacy Assessment or Random Sample Privacy Assessment at any time; and

(b) where it is subject to such a Privacy Assessment in a year in which it would otherwise have been required to carry out a Privacy Self-Assessment in accordance with Section I2.37, shall not be required to carry out that self-assessment in that year.

Privacy Self-Assessment

I2.39 I2.39 Where, in accordance with the requirements of this Section I2, an Other User is subject to a Privacy Self-Assessment in any year, that Other User shall:

(a) carry out the Privacy Self-Assessment during that year;

(b) do so in accordance with the Privacy Controls Framework; and

(c) ensure that the outcome of the Privacy Self-Assessment is documented and is submitted to the Independent Privacy Auditor for review by no later than the date which is 13 months after the date of the commencement of the previous Full Privacy Assessment or (if more recent) Privacy Self-Assessment.

Other Users: Obligation to Pay Explicit Charges

I2.40 Each Other User shall pay to the DCC all applicable Charges in respect of:

(a) all Privacy Assessments carried out in relation to it by the Independent Privacy Auditor;

(b) the production by the Independent Privacy Auditor of any Privacy Assessment Reports following such assessments; and

(c) all related activities of the Independent Privacy Auditor in respect of that Other User in accordance with this Section I2.

I2.41 Expenditure incurred in relation to Other Users in respect of the matters described in Section I2.40 shall be treated as Recoverable Costs in accordance with Section C8 (Panel Costs and Budgets).

I2.42 For the purposes of Section I2.40 the Panel shall, at such times and in respect of such periods as it may (following consultation with the DCC) consider appropriate, notify the DCC of:

(a) the expenditure incurred in respect of the matters described in Section I2.40 that is attributable to individual Other Users, in order to facilitate Explicit Charges designed to pass-through the expenditure to such Other Users pursuant to Section K7 (Determining Explicit Charges); and

(b) any expenditure incurred in respect of the matters described in Section I2.40 which cannot reasonably be attributed to an individual Other User.

J CHARGES

J1. PAYMENT OF CHARGES

Charges

J1.1 Each Party shall pay the Charges to the DCC, which Charges shall be determined in accordance with the Charging Statement applicable from time to time.

Invoicing of Charges

J1.2 Following the end of each month in which one or more Parties incurs Charges in accordance with the Charging Statement, the DCC shall prepare and submit to each such Party one or more invoices or one or more invoices with a separate accompanying statement (in either case, an "**Invoice**") showing:

(a) in respect of all Charges other than those referred to in Section J1.2(b):

(i) the date by which payment is due pursuant to Section J1.5;

(ii) a breakdown (in reasonable detail) of the Charges incurred by that Party in that month;

(iii) subject to Section J1.4, the amount of VAT payable on the above amounts;

(iv) any adjustment required pursuant to Section J1.9; and

(v) the total amount payable by that Party in respect of the above; and

(b) in respect of any Communications Hub Finance Charges which are required to be invoiced separately under the terms of a Direct Agreement with an Approved Finance Party:

(i) the date by which payment is due pursuant to Section J1.5;

(ii) a breakdown (in reasonable detail) of the Charges incurred by that Party in that month;

(iii) subject to Section J1.4, the amount of VAT payable on the above amounts;

(iv) any adjustment required pursuant to Section J1.9; and;

(v) the total amount payable by that Party in respect of the above.

J1.3 The DCC is not obliged to issue an Invoice to a Party in respect of a month under Section J1.2 where the aggregate Charges incurred by that Party in respect of that month are less than the Minimum Monthly Charge (inclusive of VAT). Where the DCC opts not to issue an Invoice to Party in respect of a month in reliance on this Section J1.3, the DCC shall carry forward the Charges incurred in respect of that month and aggregate them with the Charges incurred by that Party in respect of the following month for the purposes of Section J1.2. Notwithstanding the other provisions of this Section J1.3, the DCC must, in respect of each Party that has incurred Charges in respect of a Regulatory Year, issue at least one Invoice to that Party in respect of that Regulatory Year.

J1.4 The Charges stated in each Invoice shall be stated exclusive of VAT, which shall be added if appropriate at the rate prevailing at the relevant tax point. A Party shall only be required to pay VAT where the DCC provides an appropriate VAT invoice.

Payment of Charges

J1.5 Each Party shall pay the amount set out in an Invoice issued to it by the DCC by the "**Due Date**" for payment; being the later of:

(a) 5 Working Days following receipt of such invoice; and

(b) 8 Working Days following the end of the month to which such invoice relates.

J1.6 Without prejudice to a Party's right to dispute the Charges in accordance with Section J2 (Payment Default and Disputes), each Party shall pay the amount set out in each Invoice addressed to it by the Due Date for such payment regardless of any such dispute. Nevertheless, where the DCC agrees that an Invoice contains a manifest error, the DCC shall cancel that Invoice (which will not therefore be payable) and promptly issue a replacement Invoice.

J1.7 Payments shall be made in pounds sterling by transfer of funds to the credit of the account specified in the Invoice, and shall not be deemed to be made until the amount is available as cleared funds. Each payment shall identify within its reference the Invoice number to which that payment relates. The paying Party shall be responsible for all banking fees associated with the transfer of funds. The DCC may at its discretion specify a different account for amounts payable by way of the Communications Hub Finance Charges relating to each Approved Finance Party (separately from amounts payable in relation to each other Approved Finance Party and/or all other Charges). The accounts specified by the DCC for the purposes of amounts payable by way of the Communications Hub Finance Charges may be accounts held in the name of the relevant Approved Finance Party.

Estimation of Charges

J1.8 If any information that the DCC requires in order to prepare an Invoice is not available at the time that Invoice is prepared, then the DCC may prepare that Invoice based on its reasonable estimate of that information.

Adjustment of Charges

J1.9 Where:

(a) the DCC prepared an Invoice based on its estimate of any information, and the actual information subsequently becomes available to the DCC;

(b) there is a change to the information used by the DCC to prepare an Invoice (including following a reconciliation or amendment of Registration Data); or

(c) it is agreed (or determined), in accordance with Section J2.4 (Resolution of Payment Default), that there was an error in an Invoice,

then the DCC shall include an adjustment in the next Invoice for the relevant Party to be produced thereafter (or, where no Invoice is due to be produced, the DCC shall produce a separate Invoice for such purpose).

J1.10 Each adjustment to be included pursuant to Section J1.9 shall be:

(a) the difference between the amount included in the previous Invoice, and the amount that should have been included (being, as applicable, either an additional amount payable to the DCC, or a credit in favour of the relevant Party); plus

(b) interest on the amount of such difference calculated from day-to-day from the Due Date of the previous Invoice to (but excluding) the Due Date of the Invoice in which such adjustment is to be included (compounded monthly).

Interest Rate

J1.11 The interest rate applying for the purposes of Section J1.10 shall be the Non-Default Interest Rate.

Further Supporting Information

J1.12 The DCC shall, where requested by a Party, provide such additional information as that Party may reasonably request regarding the calculation of the Charges payable by that Party.

J2. PAYMENT DEFAULT AND DISPUTES

Notification of Payment Failure

J2.1 Where a Party fails to pay an amount set out in an Invoice by the relevant Due Date, then the DCC shall, on the Working Day following the Due Date, issue a notice to that Party:

(a) setting out the unpaid amount; and

(b) referring to the matters set out in Sections J2.2, J2.4, J2.5, J3.16 (where applicable), and M8.1(c) (Events of Default).

Default Interest

J2.2 Where a Party fails to pay an amount set out in an Invoice by the relevant Due Date, then that Party shall pay interest on that amount at the Default Interest Rate calculated from day-to-day from the Due Date to (but excluding) the date on which payment is made (compounded monthly).

Notification of Payment Disputes

J2.3 Where a Party wishes to dispute any amount set out in an Invoice addressed to it, then that Party shall nevertheless pay the full amount set out in the Invoice by the Due Date, and shall give notice to the DCC of the disputed amount and the reason for the dispute. A Party may not give notice under this Section J2.3 (or otherwise dispute an amount set out in an Invoice) more than 12 months after the Due Date for that Invoice.

Resolution of Payment Disputes

J2.4 Where a Party disputes, in accordance with Section J2.3, any amount set out in an Invoice addressed to it, then:

(a) such Party and the DCC shall each in good faith negotiate to resolve the dispute amicably and as soon as reasonably practicable after it arises;

(b) the DCC shall provide all such evidence in support of its position as the disputing Party may reasonably request, and the DCC shall provide such evidence within 5 Working Days after such request;

(c) no earlier than 1 Working Day after receipt from the DCC of the information requested under Section J2.4(b) (or, where the DCC does not comply with such request, on the expiry of the period referred to in that Section), the disputing Party may refer the dispute to the Panel, in which case each of the DCC and the disputing Party shall be entitled to provide written submissions in support of its position;

(d) where a dispute is referred to the Panel in accordance with Section J2.4(c), the Panel shall convene a meeting and determine the dispute within 10 Working Days of the reference being made (to which meeting representatives of the disputing Party and the DCC may be invited in accordance with Section C (Governance)); and

(e) where the Panel determines that there has been an overpayment to the DCC, the DCC shall include an adjustment in accordance with Section J1.9(c) to address such overpayment (or comply with any direction of the Panel to repay the relevant amount together with interest at the rate that would have applied had the adjustment been made in accordance with Section J1.9(c)).

J2.5 Section J2.4, and any determination by the Panel pursuant thereto, are without prejudice to the following rights of the Parties:

(a) where the amount set out in an Invoice addressed to a Party is disputed on the grounds of whether or not the Charges were calculated and levied in accordance with the Charging Methodology and the Charging Statement, then either of that Party or the DCC may refer the matter to the Authority for determination pursuant to Condition 20 of the DCC Licence; or

(b) where the amount set out in an Invoice addressed to a Party is disputed on any other grounds, then either of that Party or the DCC may refer the matter to arbitration in accordance with Section M7 (Dispute Resolution).

Pursuing Non-Payment

J2.6 Where the DCC has served a notice in accordance with Section J2.1 in respect of Charges payable by a Party, and such Charges have not been paid within three (3) Working Days following that notice, the DCC shall:

(a) as required by Section M8.2 (Notification of Events of Default), notify the Panel that an Event of Default has occurred in respect of that Party under Section M8.1(c); and

(b) the DCC shall take all reasonable steps and proceedings (in consultation with the Panel) to pursue and recover the unpaid amount (together with interest), and the DCC shall take all reasonable steps to gain agreement from the Panel for the DCC's approach, and the DCC shall continue with such steps and proceedings unless and until the Panel (whether on the application of the DCC or otherwise) determines that it would not be worthwhile to do so in the circumstances (having regard to, amongst other things, the DCC’s duties under part D of Condition 11 of the DCC Licence).

J2.7 Any Party may appeal the decision of the Panel under Section J2.6 to the Authority, and the DCC shall comply with any decision of the Authority in respect of such matter (which shall be final and binding, but without prejudice to the Panel's ability to make a further decision under Section J2.6 following a material change in circumstances).

Records

J2.8 Without prejudice to any other requirements under Laws or Directives, the DCC shall maintain records of each Invoice (together with reasonable supporting evidence for the Charges levied in the Invoice) for a period of at least 18 months following the date of the Invoice.

J3. CREDIT COVER REQUIREMENT

Obligation to Provide Credit Support

J3.1 Each Party shall provide Credit Support to the DCC in one or more of the following forms:

(a) a Bank Guarantee;

(b) a Letter of Credit; and/or

(c) a Cash Deposit.

J3.2 For clarity, a Parent Company Guarantee does not constitute Credit Support. However, provision of a Parent Company Guarantee alters a Party's Credit Cover Requirement calculation (see Section J3.15).

Amount of Credit Support to be Provided

J3.3 Each Party shall provide and maintain Credit Support with an aggregate value equal to or greater than that Party's Credit Cover Requirement.

J3.4 The DCC shall calculate each Party's "**Credit Cover Requirement**" from time to time (and at least once a month) as follows:

(a) the Party's Value at Risk (see Section J3.6); minus

(b) the Party's Unsecured Credit Limit (see Section J3.7),

provided that, where a Party's Credit Cover Requirement would otherwise be equal to or less than the Credit Cover Minimum Threshold, the Party's Credit Cover Requirement shall be deemed to be zero.

J3.5 Except where the Party's Credit Cover Requirement is zero (or deemed to be zero as described in Section J3.4), the DCC shall notify each Party of the Credit Cover Requirement calculated in respect of that Party (and of the Value at Risk, Maximum Credit Value, Unsecured Credit Factor Percentage, and Unsecured Credit Limit used in that calculation).

Party's Value at Risk

J3.6 Each Party's "**Value at Risk**" shall be calculated as 115% of the Charges (inclusive of VAT, but excluding any and all annual Explicit Charges) set out in the most recently produced Invoice for that Party at the time of the calculation.

Party's Unsecured Credit Limit

J3.7 Each Party's "**Unsecured Credit Limit**" is equal to:

(a) the Party's Maximum Credit Value (see Section J3.8); multiplied by

(b) the Party's Unsecured Credit Factor Percentage (see Section J3.10).

Party's Maximum Credit Value

J3.8 Each Party's "**Maximum Credit Value**" is the amount recommended by the Credit Assessment Agency as the maximum amount a creditor should have outstanding to the Party at any one time (subject to Section J3.16).

J3.9 However, where a Party has provided a Parent Company Guarantee, the Party's Maximum Credit Value shall be based on the creditworthiness of the Party's guarantor (see Section J3.15).

Party's Unsecured Credit Factor Percentage

J3.10 Each Party's "**Unsecured Credit Factor Percentage**" shall be determined in accordance with Section J3.11, J3.12, J3.13 or J3.14 (as applicable).

J3.11 If a Party has failed to pay the Charges set out in an Invoice by the Due Date on three or more occasions during the 12 months preceding the date on which the Unsecured Credit Factor Percentage is being determined, then the Party's Unsecured Credit Factor Percentage shall always be zero (and none of Sections J3.12, J3.13, and J3.14 shall apply).

J3.12 If where a Party has provided a Parent Company Guarantee, the Party's Unsecured Credit Factor Percentage shall be based on the creditworthiness of the Party's guarantor (see Section J3.16).

J3.13 Unless Section J3.12 applies, if a Party has one or more Recognised Credit Ratings, the Party's Unsecured Credit Factor Percentage shall be determined as set out in the table below (based, where the Party has more than one rating, on the lowest of the ratings):

Moody's		Fitch		Standard and Poor's		Unsecured Credit Factor (%)
Long-Term	Short-Term	Long-Term	Short-Term	Long-Term	Short-Term	
Aaa	P-1	AAA	F1+	AAA	A-1+	**50**
Aa1	P-1	AA+	F1+	AA+	A-1+	**50**
Aa2	P-1	AA	F1+	AA	A-1+	**50**
Aa2	P-1	AA-	F1+	AA-	A-1+	**50**
A1	P-1	A+	F1	A+	A-1	**20**
A2	P-1	A	F1	A	A-1	**20**
A3	P-2	A-	F2	A-	A-2	**20**
Baa1	P-2	BBB+	F2	BBB+	A-2	**10**

Baa2	P-3	BBB	F3	BBB	A-3	**9.5**
Baa3	P-3	BBB–	F3	BBB–	A-3	**9**
Ba1	-	BB+	-	BB+	-	**8.5**
Ba2	-	BB	-	BB	-	**8**
Ba3	-	BB-	-	BB-	-	**7.5**

J3.14 Unless Section J3.12 applies, if a Party does not have one or more Recognised Credit Ratings, the Party's Unsecured Credit Factor Percentage shall be determined in accordance with the following table (being the Party’s Credit Assessment Score):

Dun & Bradstreet / N2 Check Comprehensive Report	Unsecured Credit Factor (%)
5A1/	**10**
5A2/4A1	**9.5**
5A3/4A2/3A1	**9**
4A3/3A2/2A1	**8.5**
3A3/2A2/1A1	**8**
2A3/1A2/A1	**7.5**
1A3/A2/B1	**6.5**
A3/B2/C1	**5**
B3/C2/D1	**3.5**
C3/D2/E1	**1.5**
D3/E1/lower	**0**

Parent Company Guarantees

J3.15 Where a Party's obligations are guaranteed by a Parent Company Guarantee, then the Party's Credit Cover Requirement shall be calculated based on the creditworthiness of the Party's guarantor as follows:

(a) (subject to Section J3.15(b)) the Party's Unsecured Credit Limit shall be determined using:

(i) the guarantor's Maximum Credit Value – being the amount recommended by the Credit Assessment Agency as the maximum amount a creditor should have outstanding to the guarantor; and

(ii) (subject to Section J3.11) the guarantor's Unsecured Credit Factor Percentage – determined under Section J3.13 (if the guarantor has one or more Recognised Credit Ratings) or under Section J3.14 based on the guarantor's Credit Assessment Score (if the guarantor does not have one or more Recognised Credit Ratings; or

(b) if the Parent Company Guarantee is capped at an amount lower than the Party’s Value at Risk, then the Party’s Credit Cover Requirement shall be the weighted average of the amount calculated under Section J3.15(a) (based on the creditworthiness of the guarantor) and the amount calculated without regard to the creditworthiness of the guarantor (using the Party’s own Maximum Credit Value and Unsecured Credit Factor Percentage); such average to be weighted by reference to the Parent Company Guarantee cap and the amount by which the Party’s Value at Risk exceeds such cap.

Credit Assessment Reports

J3.16 The following shall apply in respect of each Party's Maximum Credit Value and (where relevant in accordance with Section J3.14) Credit Assessment Score:

(a) a revised Maximum Credit Value and (where applicable) the Credit Assessment Score in respect of a Party (and/or its guarantor) shall be obtained at least monthly;

(b) where no valid Maximum Credit Value exists in respect of a Party (or its guarantor), the Party's Maximum Credit Value shall be deemed to be zero; and

(c) where Section J3.14 applies and no valid Credit Assessment Score exists in respect of a Party (or its guarantor), the Party's Unsecured Credit Factor Percentage shall be deemed to be zero.

Increase or Decrease in Credit Cover Requirement

J3.17 On notifying a Party of its Credit Cover Requirement pursuant to Section J3.4, the DCC shall also specify the value of the Credit Support provided to the DCC by the Party at that time.

J3.18 Where the value of the Credit Support is less than the Party’s Credit Cover Requirement (by more than the lower of either 10% of the Party's Credit Cover Requirement or £1,000), then the Party shall, within two Working Days after receipt of such notification, ensure that additional Credit Support is provided to the DCC so that the aggregate value of all such Credit Support is equal to or greater than the Party’s Credit Cover Requirement.

J3.19 Where the value of the Credit Support exceeds the Party's Credit Cover Requirement (by more than the lower of either 10% of the Party's Credit Cover Requirement or £1,000), then the DCC shall, within five Working Days after a request from a Party to do so, return that Party’s Credit Support (or any part of it) to that Party; provided that the DCC shall never be obliged to return Credit Support to the extent that such return would reduce the aggregate value of the Party’s Credit Support below the Party Credit Cover Requirement.

J3.20 Additions and reductions in Credit Support pursuant to Section J3.18 and J3.19 may (without limitation) be achieved by amending the terms of existing Credit Support or exchanging Credit Support.

J3.21 For clarity, if a Bank Guarantee, Letter of Credit or Parent Company Guarantee provided on behalf of a Party ceases to satisfy the requirements of the definitions of Bank Guarantee, Letter of Credit or Parent Company Guarantee (respectively), then the value of such Credit Support or of the Party’s Unsecured Credit Factor Percentage (as applicable) shall be calculated as if no such document had been provided (and the DCC shall return such document to the Party (or as directed by the Party) within 5 Working Days after a request to do so).

Breach of Credit Cover Obligations

J3.22 Where a Party fails to provide Credit Support (or additional Credit Support) to the DCC in accordance with this Section J3, then the DCC shall, on the Working Day immediately following such failure, issue a notice to that Party:

(a) setting out the value of the Credit Support shortfall; and

(b) referring to the matters set out in Section M8.1(d) (Events of Default).

Disputes

J3.23 Where a Party disputes the amount of Credit Support requested by the DCC under this Section J3, that Party shall nevertheless provide the requested amount of Credit Support to the DCC, pending resolution of the dispute. In the case of such a dispute:

(a) the Party and the DCC shall each in good faith negotiate to resolve the dispute amicably and as soon as reasonably practicable after it arises;

(b) the DCC shall provide all such evidence in support of its position as the disputing Party may reasonably request, and the DCC shall provide such evidence within 5 Working Days after such request;

(c) no earlier than 1 Working Day after receipt from the DCC of the information requested under Section J3.23(b) (or, if the DCC does not comply with such request, on the expiry of the period referred to in that Section), the disputing Party may refer the dispute to the Panel, in which case the DCC and the disputing Party shall each be entitled to provide written submissions in support of its position;

(d) where a dispute is referred to the Panel in accordance with Section J3.23(c), the Panel shall convene a meeting and determine the dispute within 10 Working Days of the reference being made (and representatives of the disputing Party and the DCC may be invited to the meeting in accordance with Section C (Governance)); and

(e) the disputing Party and the DCC shall each give effect to any determination of the Panel pursuant to this Section J3.15, which shall be final and binding for the purposes of this Code.

Use of Credit Support

J3.24 Where a Party fails to pay the Charges set out in an Invoice addressed to that Party by the Due Date, and where the DCC has issued a notice to that Party under Section J2.1 (Notification of Payment Failure), the DCC shall (in addition to any other remedies available to it) within five Working Days following the Due Date:

(a) claim an amount equal to the unpaid Charges plus interest (or, if lower, as much as is available to be claimed) under any Bank Guarantee or Letter of Credit provided on behalf of that Party;

(b) remove an amount equal to the unpaid Charges plus interest accruing under Section J2 (or, if lower, as much as is available to be removed) from any Cash Deposit account; or

(c) undertake a combination of the above in respect of a total amount equal to the unpaid Charges plus interest (or, if lower, as much as is available to be claimed or removed).

J3.25 The DCC shall notify the Party as soon as reasonably practicable after the DCC takes any action pursuant to Section J3.24.

J3.26 The DCC shall only exercise its rights in respect of a Party's Credit Support in accordance with Section J3.24.

J3.27 Any amount received by the DCC pursuant to the exercise of its rights in respect of a Party's Credit Support shall discharge the Party's payment obligations to the extent of the amount so received, and reduce the value of the Credit Support to the same extent.

Cash Deposit

J3.28 Interest that accrues on the funds deposited in a Cash Deposit account shall be added to and form part of such deposit.

J3.29 It is agreed that all right, title and interest in and to the Cash Deposit vests in the DCC absolutely free and clear of any liens, claims, charges, encumbrances or other security interests (but without prejudice to the DCC's obligation to return an equivalent amount of money to the Party subject to and in accordance with Section J3.19).

Letters of Credit and Bank Guarantees

J3.30 Where a Party has procured that Credit Support is delivered to the DCC in the form of a Letter of Credit or Bank Guarantee, and where that Letter of Credit or Bank Guarantee has 20 Working Days or less left until it expires, the DCC shall give notice of that fact to the Party (which notice must refer to the matters set out in Section J3.31).

J3.31 Where the DCC has given notice to a Party pursuant to Section J3.30, and where the Party has not (within 10 Working Days after such notice) provided replacement Credit Support of equivalent value to the DCC (to take effect on or before expiry of the current Letter of Credit or Bank Guarantee), then the DCC shall:

(a) prior to the expiry of the Letter of Credit or Bank Guarantee, claim the entire undrawn value of the Letter of Credit or Bank Guarantee; and

(b) hold any amount so claimed as if it had been paid to the DCC as a Cash Deposit.

J4. REVIEW AND FORECASTING OF CHARGES

Review of Charges

J4.1 The Charges payable from time to time are set out in the Charging Statement applicable at that time.

J4.2 The DCC shall only amend the Charges from time to time in accordance with the DCC Licence. The DCC shall only amend the Charges once in each calendar year, such amendments to have effect from the start of each Regulatory Year (save for amendments permitted or required in accordance with Condition 19.11 of the DCC Licence). This Section J4.2 is without prejudice to the requirements of Condition 19 of the DCC Licence, and (unless the Authority gives consent under Condition 19.10 of the

DCC Licence) the DCC shall give notice of any proposed changes to Parties pursuant to Condition 19.9 of the DCC Licence.

Indicative Charging Statements

J4.3 Within the first five Working Days of April, July, October and January in each year, the DCC shall create and publish on the DCC Website an indicative Charging Statement for the first Regulatory Year due to start thereafter, setting out indicative Charges for that Regulatory Year based on the information available to the DCC at the start of the month of publication.

Indicative Budgets

J4.4 Within the first five Working Days of April, July, October and January in each year, the DCC shall create and publish on the DCC Website a budget for the second and third Regulatory Years due to start thereafter, setting out indicative figures for each such Regulatory Year based on the information available to the DCC at the start of the month of publication.

J4.5 Each such budget will contain indicative values for the following (as each such expression is defined in the Charging Methodology):

Acronym	Name
EAR_t	Estimated Allowed Revenue
EFR_t	Estimated Fixed Revenue
$EESR_t$	Estimated Elective Services Revenue
$EECR_t$	Estimated Explicit Charges Revenue
NFR_t	National Fixed Revenue
$AHFR_t$	Alt HAN Fixed Revenue
RFR_{rt}	Regional Fixed Revenue
EC_{it}	Explicit Charge for each Explicit Charging Metric
$RCHFR_{rt}$	Regional Communications Hub Fixed Revenue
$RCHDR_{hrt}$	Regional Communications Hub Device Revenue

Working Model

J4.6 The DCC shall publish a working model which allows Parties to estimate their indicative Charges based on their view of input data relevant under the Charging Methodology, and which allows Parties to test potential modifications to the Charging Methodology. The DCC shall publish such model in an open-access or off-the-shelf software format, and hereby authorises the Parties to use and modify the model for the purposes set out in this Section J4.6 (subject to the relevant software licence). Such model shall not form part of the Charging Methodology.

Invoicing Timetable

J4.7 The DCC shall, from time to time, publish an indicative timetable of the dates on which the DCC intends to submit invoices pursuant to Section J1.2.

Minimum Monthly Charge and Credit Cover Threshold

J4.8 The DCC shall publish, with the indicative Charging Statement published in January and with the actual Charging Statement for each Regulatory Year, the values of the Minimum Monthly Charge and the Credit Cover Threshold for that Regulatory Year.

K CHARGING METHODOLOGY

K1. INTRODUCTION

K1.1 This Section K constitutes the Charging Methodology that the DCC is required to have in force in accordance with the DCC Licence.

K1.2 The Charges payable to the DCC by the other Parties from time to time are those Charges set out in the Charging Statement at that time, which are payable in accordance with Section J.

K1.3 The DCC is obliged under the DCC Licence to prepare the Charging Statement in accordance with this Charging Methodology.

K1.4 This Charging Methodology is subject to modification in accordance with Section D (Modification Process), by reference to the Charging Objectives. This Section K is included in this Code in order to allow for such modification. This Section K is not intended to, and does not, create any contractual obligations between the Parties.

K1.5 This Charging Methodology provides for Fixed Charges, Fixed CH Charges, Fixed Alt HAN Charges, Explicit Charges and Elective Charges. The methodology for calculating:

(a) Fixed Charges differ as between:

(i) the UITMR Period and the COMR Period (as set out in Section K5); and

(ii) the period which falls after the COMR Period (as set out in Section K6);

(b) Fixed Alt HAN Charges differ as between:

(i) the UITMR Period; and

(ii) the period which falls during and after the COMR Period (as set out in Sections K5A, K5B and K6B respectively).

K1.6 The DCC shall act reasonably and in a manner consistent with the Charging Objectives in undertaking all calculations and estimations required pursuant to this Charging Methodology.

K1.7 The expressions used in this Charging Methodology shall have the meanings given to them in Section K11.

K2. ESTIMATED REVENUES

Estimated Allowed Revenue

K2.1 In respect of each Regulatory Year, the DCC shall estimate the Allowed Revenue for that Regulatory Year. Such estimate for each Regulatory Year shall be the "**Estimated Allowed Revenue**" for that Regulatory Year.

Estimated Elective Service Revenue

K2.2 In respect of each Regulatory Year, the DCC shall estimate the amount that will be payable to it in respect of the provision of Elective Communication Services during that Regulatory Year. Such estimation shall be based on the Charges payable under the relevant Bilateral Agreements, the DCC's estimate of the frequency at which the DCC will provide such Services (to the extent such Charges are payable on that basis), and any other relevant factors.

K2.3 The DCC's estimate in accordance with Section K2.2 for each Regulatory Year shall be the "**Estimated Elective Service Revenue**" for that Regulatory Year.

Estimated Explicit Charges Revenue

K2.4 In respect of each Regulatory Year, the DCC shall estimate the amount that will be payable to it in respect of the Explicit Charging Metrics during that Regulatory Year, based on the Explicit Charges (calculated in accordance with Section K7) and the DCC's estimate of the frequency at which the Explicit Charging Metrics will occur during that year.

K2.5 The DCC's estimate in accordance with Section K2.4 for each Regulatory Year shall be the "**Estimated Explicit Charges Revenue**" for that Regulatory Year.

Estimated Fixed Revenue

K2.6 In respect of each Regulatory Year (t), the "**Estimated Fixed Revenue**" shall be calculated as follows:

$$EFR_t = EAR_t - EESR_t - EECR_t$$

Where:

EFR_t = the Estimated Fixed Revenue for the Regulatory Year t

EAR_t = the Estimated Allowed Revenue for the Regulatory Year t

$EESR_t$ = the Estimated Elective Services Revenue for the Regulatory Year t

$EECR_t$ = the Estimated Explicit Charges Revenue for the Regulatory Year t.

K3. FIXED CHARGE, FIXED CH CHARGE AND FIXED ALT HAN CHARGE CALCULATIONS

Introduction

K3.1 The DCC will determine the Fixed Charges, the Fixed CH Charges and the Fixed Alt HAN Charges for each Regulatory Year using the Estimated Fixed Revenue determined in accordance with Section K2, which is to be translated into:

(a) Fixed Charges in accordance with Section K5 (if the Regulatory Year occurs during either the UITMR Period or the COMR Period) or Section K6 (if the Regulatory Year occurs after the COMR Period);

(b) Fixed CH Charges in accordance with Section K6A (which are payable in respect of Smart Metering Systems); and

(c) Fixed Alt HAN Charges in accordance with Sections K5A, K5B and K6B (depending upon whether the Regulatory Year occurs during the UITMR Period or during or after the COMR Period).

K3.2 The Fixed Charges and Fixed Alt HAN Charges are payable in respect of:

(a) during the UITMR Period, Mandated Smart Metering Systems for Domestic Premises and Enrolled Smart Metering Systems for Non-Domestic Premises;

(b) during the COMR Period, Mandated Smart Metering Systems for Domestic Premises, and Mandated Non-Domestic Smart Metering Systems for Non-Domestic Premises; and

(c) after the COMR Period, Enrolled Smart Metering Systems (whether for Domestic Premises or Non-Domestic Premises),

and each reference in this Section K3 (or in the definitions of defined terms used directly or indirectly in this Section K3) to '**Smart Metering Systems**' shall accordingly be construed as a reference to Mandated Smart Metering Systems, Mandated Non-Domestic Smart Metering Systems or Enrolled Smart Metering Systems (as applicable).

K3.3 As further described in this Section K3, the Fixed Charges potentially differ so as to distinguish between Smart Metering Systems for Domestic Premises and for Non-Domestic Premises, and between persons within different Charging Groups.

Domestic or Non-Domestic Premises

K3.4 The Charging Objectives require the DCC to impose Fixed Charges and Fixed CH Charges in respect of Smart Metering Systems: (a) for Domestic Premises that do not distinguish (whether directly or indirectly) between Domestic Premises located in different parts of Great Britain; and (b) for Non-Domestic Premises that do not distinguish (whether directly or indirectly) between Non-Domestic Premises located in different parts of Great Britain. However, consistent with the Charging Objectives, the methodology provides for different means of calculating the Fixed Alt HAN Charges depending upon whether a Smart Metering System is for Domestic Premises or for Non-Domestic Premises. The DCC shall estimate the numbers of Domestic Premises and Non-Domestic Premises based on Registration Data (using profile class in the case of Smart Metering Systems associated with an MPAN and market sector code in the case of Smart Metering Systems associated with an MPRN, or some other sensible proxy to the extent that the Registration Data does not readily identify whether a premises is a Domestic Premises and Non-Domestic Premises).

Cost-reflectivity

K3.5 One of the Charging Objectives is that the Charges are cost reflective (insofar as reasonably practicable in the circumstances of the case, having regard to the cost of implementing the methodology and subject to the objective referred to in Section K3.4). Consistent with the Charging Objectives, the methodology provides (subject to Section K3.4) for:

(a) the Fixed Charges in respect of a Smart Metering System to be set proportionately to the costs and expenses of providing the Services (other than the Communications Hub Services, the Elective Communication Services and the Explicit Charging Metrics) in respect of that Smart Metering System by Charging Group;

(b) the Fixed CH Charges in respect of a Smart Metering System to be set proportionately to the costs and expenses of providing the Communications Hub Services (other than the Explicit Charging Metrics) in respect of that Smart Metering System by Charging Group; and

(c) the Fixed Alt HAN Charges in respect of a Smart Metering System to be set proportionately to the costs of reimbursing AltHANCo for the Alt HAN Costs (other than the Explicit Charging Metrics) in respect of that Smart Metering System by Charging Group,

in each case as set out in the remainder of this Section K3.

Regions

K3.6 The costs and expenses of providing the Services (ignoring the Elective Communication Services and ignoring the costs and expenses designed to be recovered pursuant to the Explicit Charges) in respect of a Smart Metering System for a premises may vary depending upon the Region in which such premises is located. For the reasons described in Section K3.4, the Fixed Charges and Fixed CH Charges in respect of Smart Metering Systems will not differ by Region.

K3.7 In order to provide a degree of transparency of costs, the DCC must split the Estimated Fixed Revenue for Regulatory Year (t) between:

(a) revenue relating to the cost and expenses of providing the Services that should be recovered on a uniform basis across all the Regions (the **National Fixed Revenue**);

(b) revenue relating to the reimbursement of Alt HAN Costs (the **Alt HAN Fixed Revenue**); and

(c) revenue relating to the cost and expenses of providing the Services that should be recovered on a basis that differentiates between Regions (for each Region, the **Regional Fixed Revenue**).

K3.8 In order to provide a degree of transparency of costs, the DCC shall apportion the Estimated Fixed Revenue between:

(a) the National Fixed Revenue, the Alt HAN Fixed Revenue and the Regional Fixed Revenue for each Region so as to reflect the relative proportion of the cost and expenses that the DCC incurs across all Regions or in particular Regions in providing the Services and in reimbursing the Alt HAN Costs (ignoring the Communications Hub Services, the Test CH Services and the Elective Communication Services and ignoring the costs and expenses designed to be recovered pursuant to the Explicit Charges);

(b) the Regional Communications Hub Fixed Revenue for each Region so as to reflect the cost and expenses that the DCC incurs in providing, in respect of that Region, the Communications Hub Services and the Test CH Services (ignoring the incremental costs and expenses incurred in providing individual Communications Hubs, and also ignoring the costs and expenses designed to be recovered pursuant to the Explicit Charges); and

(c) the Regional Communications Hub Device Revenue for each Region so as to reflect the incremental cost and expenses that the DCC incurs in providing, in respect of that Region, each individual Communications Hub of each HAN Variant which is available for that Region (ignoring the costs and expenses designed to be recovered pursuant to the Explicit Charges), in each case, so that any revenue restriction correction factor adjustment contained within the Estimated Fixed Revenue is apportioned between (a), (b) or (c) above on the basis of the extent to which it arose in relation either to the Services referred to in (a), (b) or (c) respectively.

K3.9 The apportionment described in Sections K3.7 and K3.8 shall be such that:

$$EFR_t = NFR_t + AHFR_t + \sum_{\forall r} RFR_{rt} + \sum_{\forall r} RCHFR_{rt} + \sum_{\forall r \, \forall h} RCHDR_{hrt}$$

Where:

$EFR_t =$ the Estimated Fixed Revenue (estimated in accordance with Section K2) for Regulatory Year (t).

$NFR_t =$ the National Fixed Revenue (estimated in accordance with Section K3.7 and K3.8) for Regulatory Year (t).

$AHFR_t =$ the Alt HAN Fixed Revenue (estimated in accordance with Section K3.7 and K3.8) for Regulatory Year (t).

$RFR_{rt} =$ the Regional Fixed Revenue (estimated in accordance with Section K3.7 and K3.8) within each Region (r) for Regulatory Year (t).

$RCHFR_{rt} =$ the Regional Communications Hub Fixed Revenue (estimated in accordance with Section K3.7 and K3.8) within each Region (r) for Regulatory Year (t).

$RCHDR_{hrt} =$ the Regional Communications Hub Device Revenue (estimated in accordance with Section K3.7 and K3.8) for each HAN Variant (h) within each Region (r) for Regulatory Year (t).

Charging Groups

K3.10 The methodology recognises the following five categories for Smart Metering Systems. The Fixed Charges are payable by Parties in all five categories (each a **Charging Group**). The Fixed CH Charges are payable by Parties in only the first three categories (each a **CH Charging Group**). The Fixed Alt HAN Charges are payable by Parties in only the first and third categories (each an **Alt HAN Charging Group**):

(a) the Import Suppliers (**Charging Group g1**);

(b) the Export Suppliers (**Charging Group g2**);

(c) the Gas Suppliers (**Charging Group g3**);

(d) the Electricity Distributors (**Charging Group g4**); and

(e) the Gas Transporters (**Charging Group g5**).

Application of Charging Group Weighting Factors

K3.11 For the reasons described in Section K3.5, the Fixed Charges, Fixed CH Charges and Fixed Alt HAN Charges payable by each Charging Group may need to differ. This is achieved through the Charging Group, CH Charging Group and Alt HAN Charging Group Weighting Factors.

K3.12 The Weighting Factors are designed:

(a) to reflect the relative proportion of the costs and expenses likely to be incurred by the DCC in providing the Services and in reimbursing the Alt HAN Costs (ignoring the Elective Communication Services and ignoring the costs and expenses designed to be recovered pursuant to the Explicit Charges) to the persons in each Charging Group;

(b) to specify the ratio of the costs and expenses to be incurred in respect of each Smart Metering System (without regard to the number of Smart Metering Systems); and

(c) so that the sum of the Charging Group, CH Charging Group and Alt HAN Charging Group Weighting Factors shall in each case be equal to one (1).

K3.13 For Fixed Charges, the "**Charging Group Weighting Factors**" to apply to each Charging Group in respect of each Regulatory Year are to be determined by the DCC in accordance with Section K3.12, and set out in the Charging Statement for that Regulatory Year. The DCC shall make such determination based on its estimate of the demand of persons within each Charging Group for each of the Services other than the Elective Communication Services. Prior to the start of the UITMR Period, such estimates of demand will be based on assumptions for the Regulatory Year starting on 1st April 2021. Once data on usage becomes available the estimates will be determined as the average of the previous two full Regulatory Years of actual data plus the DCC's forecasts for the two Regulatory Years ahead.

K3.14 For Fixed CH Charges, the "**CH Charging Group Weighting Factors**" to apply to each CH Charging Group in respect of each Regulatory Year are to be determined by the DCC on the basis of the relative proportion of their Charging Group Weighting Factors, such that:

$$\beta_{gt} = \frac{\alpha_{gt}}{\sum\limits_{g=1 \Box 3 \Box} \alpha_{gt}}$$

Where:

β_{gt} = = the CH Charging Group Weighting Factor for applicable to Regulatory Year (t) and each Charging Group (g)

α_{gt} = = the Charging Group Weighting Factor applicable to Regulatory Year (t) and each Charging Group (g).

K3.15 For Fixed Alt HAN Charges, the **"Alt HAN Charging Group Weighting Factors"** to apply to each Alt HAN Charging Group in respect of each Regulatory Year are to be determined by the DCC on the basis of an expectation of equal use of Alt HAN services per Enrolled Smart Metering System by Import Suppliers and Gas Suppliers, such that:

γ_{gt} 0.5 where g =1 or 3

γ_{gt} 0 where g =2, 4 or 5.

Where:

γ_{gt} = the Alt HAN Charging Group Weighting Factor for applicable to Regulatory Year (t) and each Charging Group (g).

Determining the Fixed Charges

K3.15A In determining the Fixed Charges, the DCC shall have regard to the need, for the purposes of making a prudent estimate in accordance with Condition 36.5 of the DCC Licence, to provide for the availability at all times of a contingency fund in respect of the 4G DBT Finance Charges relating to each Communications Hub Finance Facility that is equal to the DCC's estimate of three months of the 4G DBT Finance Costs relating to that facility.

Determining Fixed CH Charges

K3.16 In determining the Fixed CH Charges, the DCC shall have regard to the need, for the purposes of making a prudent estimate in accordance with Condition 36.5 of the DCC Licence, to provide for the availability at all times of a contingency fund in respect of the Communications Hub Finance Charges relating to each Communications Hub Finance Facility that is equal to the DCC's estimate of three months of the Communications Hub Finance Costs relating to that facility.

Description of Approach to Determining Fixed Alt HAN Charges for Smart Metering Systems for Domestic Premises and Non-Domestic Premises during the UITMR Period and during and after the COMR Period

K3.17 The "**Alt HAN Cost Domestic Allocation**" is a factor between zero and one that is determined by the DCC based on information provided by AltHANCo to reflect the proportion of usage of Alt HAN Equipment in Domestic Premises expressed as a fraction of the total usage across both Domestic Premises and Non-Domestic Premises and is represented by *t* for Regulatory Year (t) such that:

$$\mu_t = \frac{DAHU_t}{DAHU_t + NAHU_t}$$

Where:

$DAHU_t$ is the number of MPANs and MPRNs associated with the use of Alt HAN Equipment in Domestic Premises, derived by the DCC from the data provided to it by AltHANCo in accordance with Section Z4.35 (Provision of Information to the DCC) and available to it one month prior to the issue of the most recent Charging Statement and the Registration Data prevailing at that time.

$NAHU_t$ is the number of MPANs and MPRNs associated with the use of Alt HAN Equipment in Non-Domestic Premises, derived by the DCC from the data provided to it by AltHANCo in accordance with Section Z4.35 (Provision of Information to the DCC) and available to it one month prior to the issue of the most recent Charging Statement and the Registration Data prevailing at that time.

K4. NO LONGER USED

K5. DETERMINING FIXED CHARGES DURING THE UITMR PERIOD AND DURING THE COMR PERIOD

Introduction

K5.1 The DCC will determine the Fixed Charges for each Regulatory Year during the UITMR Period and during the COMR Period in accordance with this Section K5, using:

(a) the National Fixed Revenue, the Regional Fixed Revenue and the Regional Communications Hub Fixed Revenue for that Regulatory Year determined in accordance with Section K3;

(b) (in the case of the UITMR Period only) an estimate, in accordance with this Section K5, of the number of Smart Metering Systems for Non-Domestic Premises that will have been (and remain) Enrolled as at the beginning of that Regulatory Year;

(c) an estimate, in accordance with this Section K5, of the number of Mandated Smart Metering Systems for Domestic Premises that will exist as at the beginning of that Regulatory Year;

(d) the Charging Group Weighting Factors and other relevant matters described in Section K3; and

(e) (in the case of the COMR Period only) an estimate, in accordance with this Section K5, of the number of Mandated Non-Domestic Smart Metering Systems for Non-Domestic Premises that will exist as at the beginning of that Regulatory Year.

Estimates: Non-Domestic Premises (UITMR Period)

K5.2 In respect of Regulatory Years occurring during the UITMR Period:

(a) the DCC must estimate the total number of Smart Metering Systems for Non- Domestic Premises that will have been (and remain) Enrolled as at the beginning of that Regulatory Year;

(b) the DCC must estimate the number of persons in each Charging Group for such Smart Metering Systems;

(c) the DCC must break down its estimate pursuant to Section K5.2(b) by reference to the number of Smart Metering Systems in each Region; and

(d) the estimate pursuant to Section K5.2(c) in respect of a Regulatory Year (t), each Charging Group (g) and each Region (r), shall be represented as $RENSMS_{grt}$.

Estimates: Non-Domestic Premises (COMR Period)

K5.2A In respect of Regulatory Years occurring during the COMR Period:

(a) the DCC must estimate the aggregate number of Mandated Non-Domestic Smart Metering Systems that will exist as at the beginning of that Regulatory Year;

(b) the DCC must estimate the number of persons in each Charging Group for such Mandated Non-Domestic Smart Metering Systems;

(c) the DCC must break down its estimate pursuant to Section K5.2A(b) by reference to the number of Mandated Non-Domestic Smart Metering Systems in each Region; and

(d) the estimate pursuant to Section K5.2A(c) in respect of a Regulatory Year (t), each Charging Group (g) and each Region (r), shall be represented as $RENSMS_{grt}$.

Estimates: Domestic Premises

K5.3 In respect of Regulatory Years occurring during the UITMR Period and the COMR Period:

(a) the DCC must estimate the aggregate number of Mandated Smart Metering Systems that will exist as at the beginning of that Regulatory Year;

(b) the DCC must estimate the number of persons in each Charging Group for such Mandated Smart Metering Systems;

(c) the DCC must break down its estimate pursuant to Section K5.3(b) by reference to the number of Mandated Smart Metering Systems in each Region; and

(d) the estimate pursuant to Section K5.3(c) in respect of a Regulatory Year (t), each Charging Group (g) and each Region (r), shall be represented as .$REDSMS_{grt}$.

Determining the Fixed Charges

K5.4 For each Regulatory Year (t), the DCC will determine the Fixed Charge payable in respect of each month (or part month) of Regulatory Year (t) by each person within each Charging Group (g) in respect of:

(a) (during the UITMR Period) each Enrolled Smart Metering System for a Non-Domestic Premises; or

(b) (during the COMR period) each Mandated Non-Domestic Smart Metering System for a Non-Domestic Premises; and

(c) (in either case) each Mandated Smart Metering System for a Domestic Premises (RFC_{gt}), as follows:

$$RFC_{gt} = \frac{\left(NFR_t + \sum_{\forall r} RFR_{rt}\right)}{NM_t} \times \frac{\alpha_{gt}}{\sum_{\forall g}\left(\alpha_{gt} \times \sum_{\forall r} RESMS_{grt}\right)} + \frac{\sum_{\forall r} RCHFR_{rt}}{NM_t} \times \frac{\beta_{gt}}{\sum_{\forall g}\left(\beta_{gt} \times \sum_{\forall r} RESMS_{grt}\right)}$$

Where:

α_{gt} =the Charging Group Weighting Factor (as set out in Section K3) applicable to Regulatory Year (t) and each Charging Group (g)

β_{gt} =the CH Charging Group Weighting Factor (as set out in Section K3) applicable to Regulatory Year (t) and each Charging Group (g)

NM_t =the number of months (or part months) in Regulatory Year (t)

NFR_t =the National Fixed Revenue (estimated in accordance with Section K3) for Regulatory Year (t)

RFR_{rt} =the Regional Fixed Revenue (estimated in accordance with Section K3) for Regulatory Year (t) and Region (r)

$RCHFR_{rt}$ = the Regional Communications Hub Fixed Revenue (estimated in accordance with Section K3) for Regulatory Year (t) and Region (r)

$$\forall g \forall r \quad RESMS_{grt} = REDSMS_{grt} + RENSMS_{grt}$$

$RENSMS_{grt}$ = either:

i. (during the UITMR Period) the estimate pursuant to Section K5.2(d) for Regulatory Year (t), each Charging Group (g) and each Region (r); or

ii. (during the COMR Period) the estimate pursuant to Section K5.2A(d) for Regulatory Year (t), each Charging Group (g) and each Region (r).

$REDSMS_{grt}$ = the estimate pursuant to Section K5.3(d) for Regulatory Year (t), each Charging Group (g) and each Region (r).

K5.5 [Not used]

(UITMR Period only) Calculating number of ESMSs for Fixed Charge Payment: Non-Domestic Premises

K5.6 Following the end of each month (or part month) occurring during each Regulatory Year during the UITMR Period, the DCC will:

(a) determine the actual number of Smart Metering Systems for Non-Domestic Premises that have been (and remain) Enrolled as at the end of the 15th day of that month (or, in the case of a part month that ends on or prior to the 15th day of that month, at the end of that part month), whether Enrolled during that month or previously;

(b) calculate the number of persons within each Charging Group for those Enrolled Smart Metering Systems; and

(c) break down these calculations by reference to each Party.

K5.7 The calculations in accordance with Section K5.6 of the number of Enrolled Smart Metering Systems for Non-Domestic Premises as at the end of each month (m) during Regulatory Year (t) within each Charging Group (g) broken down by reference to each Party (p), shall be represented as $\mathrm{ANSMS}_{\mathrm{pgmt.}}$

Calculating number of MSMSs for Fixed Charge Payment: Domestic Premises

K5.8 Following the end of each month (or part month) occurring during each Regulatory Year during the UITMR Period and during the COMR Period, the DCC will:

(a) determine (insofar as it is able) the actual number of Mandated Smart Metering Systems for Domestic Premises as at the end of the 15th day of that month (or, in the case of a part month that ends on or prior to the 15th day of that month, at the end of that part month);

(b) calculate the number of persons within each Charging Group for those Mandated Smart Metering Systems; and

(c) break down these calculations by reference to each Party.

K5.9 The calculations in accordance with Section K5.8 of the number of Mandated Smart Metering Systems as at the end of each month (or part month) (m) during Regulatory Year (t) within each Charging Group (g) broken down by reference to each Party (p) shall be represented as $ADSMS_{pgmt}$.

(COMR Period only) Calculating number of MNSMSs for Fixed Charge Payment: Non-Domestic Premises

K5.10 Following the end of each month (or part month) occurring during each Regulatory Year during the COMR Period, the DCC will:

(a) determine (insofar as it is able) the actual number of Mandated Non-Domestic Smart Metering Systems for Non-Domestic Premises as at the end of the 15th day of that month (or, in the case of a part month that ends on or prior to the 15th day of that month, at the end of that part month);

(b) calculate the number of persons within each Charging Group for those Mandated Non-Domestic Smart Metering Systems; and

(c) break down these calculations by reference to each Party.

K5.11 The calculations in accordance with Section K5.10 of the number of Mandated Non-Domestic Smart Metering Systems as at the end of each month (or part month) (m) during Regulatory Year (t) within each Charging Group (g) broken down by reference to each Party (p) shall be represented as $ANSMS_{pgmt}$.

K5A DETERMINING FIXED ALT HAN CHARGES DURING THE UITMR PERIOD

Introduction

K5A.1 The DCC will determine the Fixed Alt HAN Charges for each Regulatory Year during the UITMR Period in accordance with this Section K5A, using:

(a) the Alt HAN Fixed Revenue for that Regulatory Year estimated in accordance with Section K3;

(b) an estimate, in accordance with Section K5, of the number of Smart Metering Systems for Non-Domestic Premises that will have been (and remain) Enrolled as at the beginning of that Regulatory Year;

(c) an estimate, in accordance with Section K5, of the number of Mandated Smart Metering Systems for Domestic Premises that will exist as at the beginning of that Regulatory Year; and

(d) the Alt HAN Charging Group Weighting Factors and other relevant matters described in Section K3.

Determining the Fixed Alt HAN Charges (UITMR Period)

K5A.2 For each Regulatory Year (t), the DCC will determine the Fixed Alt HAN Charges payable in respect of each month (or part month) of Regulatory Year (t) by each person within each Alt HAN Charging Group (g) in respect of each Mandated Smart Metering System and each Enrolled Smart Metering System for a Non-Domestic Premises (*RAHFCgt*), as follows:

$$RAHFC_{gt} = \frac{AHFR_t}{NM_t} \times \frac{\gamma_{gt}}{\sum_{\forall g}\left(\gamma_{gt} \times \sum_{\forall r} RESMS_{grt}\right)}$$

Where:

γ_{gt} =the Alt HAN Charging Group Weighting Factor (as set out in Section K3) applicable to Regulatory Year (t) and each Charging Group (g);

NM_t =the number of months (or part months) in Regulatory Year (t);

$AHFR_t$ =the Alt HAN Fixed Revenue (estimated in accordance with Section K3) for Regulatory Year (t);

$\forall g \forall r \quad RESMS_{grt} = REDSMS_{grt} + RENSMS_{grt}$

$RENSMS_{grt}$ = the estimate pursuant to Section K5.2(d) for Regulatory Year (t), each Charging Group (g) and each Region (r);

$REDSMS_{grt}$ = the estimate pursuant to Section K5.3(d) for Regulatory Year (t), each Charging Group (g) and each Region (r).

K5B DETERMINING FIXED ALT HAN CHARGES DURING THE COMR PERIOD

Introduction

K5B.1 The DCC will determine the Fixed Alt HAN Charges for each Regulatory Year during the COMR Period in accordance with this Section K5B, using:

(e) the Alt HAN Fixed Revenue for that Regulatory Year estimated in accordance with Section K3;

(f) an estimate, in accordance with Section K5, of the number of Mandated Non-Domestic Smart Metering Systems for Non-Domestic Premises that will exist as at the beginning of that Regulatory Year;

(g) an estimate, in accordance with Section K5, of the number of Mandated Smart Metering Systems for Domestic Premises that will exist as at the beginning of that Regulatory Year; and

(h) the Alt HAN Charging Group Weighting Factors and other relevant matters described in Section K3.

Determining the Fixed Alt HAN Charges (COMR Period)

K5B.2 For each Regulatory Year (t), the DCC will determine the Fixed Alt HAN Charges payable in respect of each month (or part month) of Regulatory Year (t) by each person within each Alt HAN Charging Group (g) in respect of each Mandated Smart Metering System and each Mandated Non-Domestic Smart Metering System $(RAHFC_{gt})$, as follows:

$$RAHFC_{gt} = \frac{AHFR_t}{NM_t} \times \frac{\gamma_{gt}}{\sum_{\forall g}\left(\gamma_{gt} \times \sum_{\forall r} RESMS_{grt}\right)}$$

Where:

γ_{gt} = the Alt HAN Charging Group Weighting Factor (as set out in Section K3) applicable to Regulatory Year (t) and each Charging Group (g);

NM_t = the number of months (or part months) in Regulatory Year (t);

$AHFR_t$ = the Alt HAN Fixed Revenue (estimated in accordance with Section K3) for Regulatory Year (t);

$$\forall g \forall r \quad RESMS_{grt} = REDSMS_{grt} + RENSMS_{grt}$$

$RENSMS_{grt}$ = the estimate pursuant to Section K5.2A(d) for Regulatory Year (t), each Charging Group (g) and each Region (r);

$REDSMS_{grt}$ = the estimate pursuant to Section K5.3(d) for Regulatory Year (t), each Charging Group (g) and each Region (r).

K6. DETERMINING FIXED CHARGES AFTER THE COMR PERIOD (ENDURING)

Introduction

K6.1 The DCC will determine the Fixed Charges for each Regulatory Year following the COMR Period in accordance with this Section K6, using:

(a) the National Fixed Revenue, the Regional Fixed Revenue and the Regional Communications Hub Fixed Revenue for that Regulatory Year determined in accordance with Section K3;

(b) an estimate, in accordance with this Section K6, of the number of Smart Metering Systems that will have been (and remain) Enrolled as at the beginning of that Regulatory Year; and

(c) the Charging Group Weighting Factors and other relevant matters described in Section K3.

Estimates

K6.2 In respect of Regulatory Years occurring after the COMR Period, the DCC will estimate the number of Smart Metering Systems that will have been (and remain) Enrolled as at the beginning of that Regulatory Year. The DCC shall undertake such estimates for Domestic Premises and Non-Domestic Premises separately (being *EDSMS* and *ENSMS* respectively). For each such Regulatory Year (t), the DCC will estimate the average number of persons within each Charging Group (g) for such Smart Metering Systems, and break down such estimates by reference to the Region (r) in which the premises is located, such that:

$$\forall g \forall r \quad ESMS_{grt} = EDSMS_{grt} + ENSMS_{grt}$$

Where:

$EDSMS_{grt}$ = the DCC’s estimate of the number of persons within each Charging Group (g) for Smart Metering Systems for Domestic Premises that will have been (and remain) Enrolled as at the beginning of that Regulatory Year (t), broken down by Region (r); and

$ENSMS_{grt}$ = the DCC’s estimate of the number of persons within each Charging Group (g) for Smart Metering Systems for Non-Domestic Premises that will have been (and remain) Enrolled as at the beginning of that Regulatory Year (t), broken down by Region (r).

Determining the Fixed Charges

K6.3 For each Regulatory Year (t), the DCC will determine the Fixed Charge payable in respect of each month (or part month) of Regulatory Year (t) by each person within each Charging Group (g) in respect of each Enrolled Smart Metering System for a Non-Domestic Premises and for a Domestic Premises (EFCgt) as follows:

$$EFC_{gt} = \frac{\left(NFR_t + \sum_{\forall r} RFR_{rt}\right)}{NM_t} \times \frac{\alpha_{gt}}{\sum_{\forall g}\left(\alpha_{gt} \times \sum_{\forall r} ESMS_{grt}\right)} + \frac{\sum_{\forall r} RCHFR_{rt}}{NM_t} \times \frac{\beta_{gt}}{\sum_{\forall g}\left(\beta_{gt} \times \sum_{\forall r} ESMS_{grt}\right)}$$

Where:

α_{gt} =the Charging Group Weighting Factor (as set out in Section K3) applicable to Regulatory Year (t) and each Charging Group (g)

β_{gt} =the CH Charging Group Weighting Factor (as set out in Section K3) applicable to Regulatory Year (t) and each Charging Group (g)

NM_t =the number of months (or part months) in Regulatory Year (t)

NFR_t =the National Fixed Revenue (determined in accordance with Section K3_ for Regulatory Year (t)

$ESMS_{grt}$ = the estimated number of persons within each Charging Group (g) for Enrolled Smart Metering Systems determined in accordance with Section K6.2 for Regulatory Year (t) and each Region (r)

RFR_{rt} = the Regional Fixed Revenue (determined in accordance with Section K3) for Regulatory Year (t) and each Region (r)

$RCHFR_{rt}$ = the Regional Communications Hub Fixed Revenue (estimated in accordance with Section K3) for Regulatory Year (t) and Region (r)

K6.4 [Not used]

Calculating number of ESMSs for Fixed Charge Payment

K6.5 Following the end of each month (or part month) during each Regulatory Year occurring after the COMR Period, the DCC will:

(a) determine the actual number of Smart Metering Systems that have been (and remain) Enrolled as at the end of the 15th day of that month (or, in the case of a part month that ends on or prior to the 15th day of that month, at the end of that part month), whether Enrolled during that month or previously, and shall do so for Domestic Premises and for Non-Domestic Premises separately;

(b) calculate the number of persons within each Charging Group for such Enrolled Smart Metering Systems; and

(c) break down these calculations by reference to Parties (p), and (in the case of Smart Metering Systems for Non-Domestic Premises only) by reference to the Region in which such premises are located.

K6.6 The calculations in accordance with Section K6.5 of the number of Enrolled Smart Metering Systems as at the end of each month (or part month) (m) during Regulatory Year (t) within each Charging Group (g) broken down by reference to each Party (p), and (in the case of Non-Domestic Premises only) by reference to each Region (r), shall:

(a) in respect of Domestic Premises, be represented as $\mathrm{ADSMS}_{\mathrm{pgmt}}$; and

(b) in respect of Non-Domestic Premises, be represented as $\mathrm{ANSMS}_{\mathrm{pgrmt}}$.

K6A DETERMINING FIXED CH CHARGES

Introduction

K6A.1 The DCC will determine the Fixed CH Charges for each Regulatory Year during the UITMR Period or during or after the COMR Period in accordance with this Section K6A, using:

(a) the Regional Communications Hub Device Revenue for that Regulatory Year determined in accordance with Section K3;

(b) an estimate, in accordance with this Section K6A, of the average number of Smart Metering Systems that there will be during that Regulatory Year; and

(c) the CH Charging Group Weighting Factors and other relevant matters described in Section K3.

Estimates

K6A.2 In respect of each Regulatory Year occurring during the UITMR Period or during or after the COMR Period, the DCC will estimate the average number of Smart Metering Systems that there will be during the Regulatory Year. The DCC shall undertake such estimates for Domestic Premises and Non-Domestic Premises separately (being *EDCH* and *ENCH* respectively). For each such Regulatory Year (t), the DCC will estimate the average number of persons within each CH Charging Group (g) for such Smart Metering Systems, and break down such estimates by reference to the Region (r) in which the premises is located and the HAN Variant (h) forming part of each such Smart Metering System, such that:

$$\forall g \forall r \forall h \; ECH_{ghrt} = EDCH_{ghrt} + ENCH_{ghrt}$$

Where:

$EDCH_{ghrt}$ = the DCC’s estimate of the average number of persons within each CH Charging Group (g) for Smart Metering Systems for Domestic Premises during that Regulatory Year (t), broken down by Region (r) and HAN Variant (h); and

$ENCH_{ghrt}$ = the DCC’s estimate of the average number of persons within each CH Charging Group (g) for Smart Metering Systems for Non-Domestic Premises during that Regulatory Year (t), broken down by Region (r) and HAN Variant (h).

Determining the Fixed CH Charges

K6A.3 For each Regulatory Year (t), the DCC will determine the Fixed CH Charge payable in respect of each month (or part month) of Regulatory Year (t) by each person within each CH Charging Group (g) in respect of each Smart Metering System incorporating each HAN Variant (h) for a Non-Domestic Premises or for a Domestic Premises $(\mathrm{CHC}_{\mathrm{ght}})$ as follows:

Where:

$$CHC_{ght} = \frac{\sum_{\forall r} RCHDR_{hrt}}{NM_t} \times \frac{\beta_{gt}}{\sum_{\forall g}\left(\beta_{gt} \times \sum_{\forall r} ECH_{ghrt}\right)}$$

β_{gt} =the CH Charging Group Weighting Factor (as set out in Section K3) applicable to Regulatory Year (t) and each Charging Group (g)

NM_t =the number of months (or part months) in Regulatory Year (t)

$\mathrm{RCHDR}_{\mathrm{hrt}}$ = the Regional Communications Hub Device Revenue (determined in accordance with Section K3) for Regulatory Year (t), HAN Variant (h) and Region (r)

$\mathrm{ECH}_{\mathrm{ghrt}}$ = the estimated number of persons within each Charging Group (g) for Smart Metering Systems determined in accordance with Section K6A.2 for Regulatory Year (t), HAN Variant (h) and each Region (r).

K6A.4 [Not used]

Calculating number of CHs for Fixed CH Charge Payment

K6A.5 Following the end of each month (or part month) during each Regulatory Year occurring during the UITMR Period or during or after the COMR Period, the DCC will:

(d) determine the actual number of Smart Metering Systems that there are as at the end of the 15th day of that month (or, in the case of a part month that ends on or prior to the 15th day of that month, at the end of that part month), and shall do so for Domestic Premises and for Non-Domestic Premises separately;

(e) calculate the number of persons within each CH Charging Group for such Smart Metering Systems; and

(f) break down these calculations by reference to Parties (p), and (for transparency in the case of Smart Metering Systems for Non-Domestic Premises only) by reference to the Region in which such premises are located.

K6A.6 The calculations in accordance with Section K6A.5 of the number of Smart Metering Systems as at the end of each month (or part month) (m) during Regulatory Year (t) within each Charging Group (g) broken down by reference to each Party (p), and (for transparency in the case of Non-Domestic Premises only) by reference to each Region (r) and HAN Variant (h), shall:

(g) in respect of Domestic Premises, be represented as $\mathrm{ADCH}_{\mathrm{pghmt}}$; and

(h) in respect of Non-Domestic Premises, be represented as $\mathrm{ANCH}_{\mathrm{pgrhmt}}$.

K6B DETERMINING FIXED ALT HAN CHARGES AFTER THE COMR PERIOD (ENDURING)

K6B.1 The DCC will determine the Fixed Alt HAN Charges for each Regulatory Year after the COMR Period in accordance with this Section K6B, using:

(i) the Alt HAN Fixed Revenue, for that Regulatory Year estimated in accordance with Section K3;

(j) an estimate, in accordance with Section K6, of the number of Smart Metering Systems that there will have been (and remain) Enrolled at the beginning of that Regulatory Year; and

(k) the Alt HAN Charging Group Weighting Factors and other relevant matters described in Section K3.

Determining the Alt HAN Fixed Charges: Domestic

K6B.2 For each Regulatory Year (t) following the COMR Period, the DCC will determine the Alt HAN Fixed Charges payable in respect of each month (or part month) of Regulatory Year (t) by each person within each Alt HAN Charging Group (g) in respect of each Enrolled Smart Metering System for a Domestic Premises (*DAHFCgt*) as follows:

$$DAHFC_{gt} = \frac{AHFR_t}{NM_t} \times \frac{\mu_t \times \gamma_{gt}}{\sum_{\forall g}\left(\gamma_{gt} \times \sum_{\forall r} EDSMS_{grt}\right)}$$

Where:

μ_t =the Alt HAN Central Cost Domestic Allocation applicable to Regulatory Year (t) (set out in Section K3);

γ_{gt} =the Alt HAN Charging Group Weighting Factor (as set out in Section K3) applicable to Regulatory Year (t) and each Charging Group (g);

NM_t =the number of months (or part months) in Regulatory Year (t);

$EDSMS_{grt}$ =the estimated number of persons within each Charging Group (g) for Enrolled Smart Metering Systems for Domestic Premises determined in accordance with Section K6.2 for Regulatory Year (t) and each Region (r);

$AHFR_t$ =the Alt HAN Fixed Revenue (estimated in accordance with Section K3) for Regulatory Year (t).

Determining the Alt HAN Fixed Charges: Non-Domestic

K6B.3 For each Regulatory Year (t) following the COMR Period, the DCC will determine the Alt HAN Fixed Charges payable in respect of each month (or part month) of Regulatory Year (t) by each person within each Alt HAN Charging Group (g) in respect of each Enrolled Smart Metering System for a Non-Domestic Premises $(NAHFC_{gt})$ as follows:

$$NAHFC_{gt} = \frac{AHFR_t}{NM_t} \times \frac{(1-\mu_t)\times\gamma_{gt}}{\sum_{\forall g}\left(\gamma_{gt} \times \sum_{\forall r} ENSMS_{grt}\right)}$$

Where:

μ_t =the Alt HAN Central Cost Domestic Allocation (set out in Section K3);

γ_{gt} =the Alt HAN Charging Group Weighting Factor (as set out in Section K3) applicable to Regulatory Year (t) and each Charging Group (g);

NM_t =the number of months (or part months) in Regulatory Year (t);

$ENSMS_{grt}$ =the estimated number of persons within each Alt HAN Charging Group (g) for Enrolled Smart Metering Systems for Non-Domestic Premises determined in accordance with Section K6.2 for Regulatory Year (t) and each Region (r);

$AHFR_t$ =the Alt HAN Fixed Revenue (estimated in accordance with Section K3) for Regulatory Year (t).

K7. DETERMINING EXPLICIT CHARGES

Introduction

K7.1 The Explicit Charges for each Regulatory Year are payable in respect of the Explicit Charging Metrics for that Regulatory Year.

K7.2 The Explicit Charging Metrics from time to time are as set out in this Section K7.

K7.3 Part of the rationale for Explicit Charging Metrics is to allow the DCC to closely reflect the charges it pays to the DCC Service Providers in respect of certain services, to SECCo in respect of certain Recoverable Costs, and to AltHANCo in respect of the Alt HAN Costs, so as to minimise the risks for the DCC associated with uncertainty regarding the frequency with which such services are to be provided or such Alt HAN Costs are incurred. The Explicit Charging Metrics may comprise any or all of the Core Communication Services and of the Enabling Services (so they are a sub-set of all Services other than the Elective Communication Services) and of the Alt HAN Costs. The Explicit Charging Metrics represent those Core Communication Services, Enabling Services and Alt HAN Costs that are to be charged for separately from the Fixed Charges, Fixed CH Charges and Fixed Alt HAN Charges.

K7.4 The DCC will determine the Explicit Charges for each Regulatory Year in accordance with this Section K7.

Explicit Charging Metrics

K7.5 The Explicit Charging Metrics for each Party and the Charging Period for each month are as follows:

(a) ('*security assessments*') an obligation to pay arising during that Charging Period in respect of that Party pursuant to Section G8.51 (Users: Obligation to Pay Charges) in relation to User Security Assessments, Follow-up Security Assessments, User Security Assessment Reports or the activities of the Independent Security Assurance Service Provider;

(b) ('*privacy assessments*') an obligation to pay arising during that Charging Period in respect of that Party pursuant to Section I2.40 (Users: Obligation to Pay Charges) in relation to Full Privacy Assessments, Random Sample Privacy Assessments, Privacy Assessment Reports or the activities of the Independent Privacy Auditor;

(c) ('*LV gateway connection*') an obligation to pay arising during that Charging Period in accordance with an offer for a DCC Gateway LV Connection accepted by that Party pursuant to Section H15 (DCC Gateway Connections), including where the obligation to pay is preserved under Section H15.19(b) (Ongoing Provision of a DCC Gateway Connection);

(d) ('*HV gateway connection*') an obligation to pay arising during that Charging Period in accordance with an offer for a DCC Gateway HV Connection accepted by that Party pursuant to Section H15 (DCC Gateway Connections), including where the obligation to pay is preserved under Section H15.19(b) (Ongoing Provision of a DCC Gateway Connection);

(e) ('*gateway equipment relocation*') an obligation to pay arising during that Charging Period as a result of a request by that Party to relocate DCC Gateway Equipment under Section H15.27 (DCC Gateway Equipment);

(f) ('*elective service evaluations*') an obligation to pay arising during that Charging Period under the terms and conditions accepted by that Party for a Detailed Evaluation in respect of potential Elective Communication Services pursuant to Section H7.8 (Detailed Evaluations of Elective Communication Services);

(g) ('*P&C support*') an obligation to pay arising during that Charging Period under the terms and conditions accepted by that Party in relation to that Party's use or implementation of the Parse and Correlate Software pursuant to Section H11.12 (Provision of Support & Assistance to Users);

(h) ('*SM WAN for testing*') an obligation to pay arising during that Charging Period from the acceptance by that Party of the charges offered by the DCC to provide a connection to a simulation of the SM WAN pursuant to Section H14.31 (Device and User System Testing);

(i) ('*additional testing support*') an obligation to pay arising during that Charging Period from the acceptance by that Party of the charges offered by the DCC to provide additional testing support to that Party pursuant to Section H14.33 (Device and User System Testing);

(j) ('*communication services*') the number of each of the Services identified in the DCC User Interface Services Schedule which have been provided to that Party during that Charging Period;

(k) ('*CH non-standard delivery*') an obligation to pay arising during that Charging Period as a result of the request by that Party for non-standard Communications Hub Product delivery requirements pursuant to Section F6.17 (Non-Standard Delivery Options);

(l) ('*CH stock level charge*') the number (to be measured at the end of that Charging Period) of Communications Hubs that have been delivered to that Party under Section F6 (Delivery and Acceptance of Communications Hubs) or that have been transferred to that Party under Section F6A (Transferring Communications Hubs Between Parties) and for which none of the following has yet occurred: (i) identification on the Smart Metering Inventory as 'installed not commissioned' or 'commissioned'; (ii) rejection in accordance with Section F6.10 (Confirmation of Delivery);
(iii) delivery to the DCC in accordance with Section F8 (Removal and Return of Communications Hubs); (iv) notification to the DCC in accordance with Section F8 (Removal and Return of

Communications Hubs) that the Communications Hub has been lost or destroyed; or (v) transfer to another Party under Section F6A (Transferring Communications Hubs Between Parties);

(m) (*'GFI Testing'*) the number of each of the types of GFI Testing tools which have been delivered to that Party during that Charging Period under Section H14 (Testing Services) and in accordance with Section 15 of Appendix J (Enduring Testing Approach Document);

(n) ('*CH auxiliary equipment*') the number of each of the types of Communications Hub Auxiliary Equipment which have been delivered to that Party during that Charging Period under Section F6 (Delivery and Acceptance of Communications Hubs), and which have not been (and are not) rejected in accordance with Section F6.10 (Rejected Communications Hub Products) or (in the case of the Communications Hub Auxiliary Equipment to which Section F7.9 or F7.10 or both applies (Ownership of and Responsibility for Communications Hub Auxiliary Equipment)) returned, or notified as lost or destroyed, for a reason which is a CH Pre-Installation DCC Responsibility;

(o) ('*CH returned and redeployed*') the number of Communications Hubs which have been returned by that Party during that Charging Period for a reason which is a CH User Responsibility, and which have been (or are intended to be) reconditioned for redeployment pursuant to Section F8 (Removal and Return of Communications Hubs);

(p) ('*CH returned not redeployed*') the number of Communications Hubs which have been returned, or notified as lost or destroyed, by that Party during that Charging Period for a reason which is a CH User Responsibility, and which have not been (and are not intended to be) reconditioned for redeployment pursuant to Section F8 (Removal and Return of Communications Hubs);

(q) ('*CH wrong returns location*') an obligation to pay arising during that Charging Period as a result of the return by that Party of Communications Hubs to the wrong returns location as referred to in Section F8.9 (Return of Communications Hubs);

(r) ('*test comms hubs*') the number of Test Communications Hubs delivered to that Party during that Charging Period, and which have not been (and are not) returned to the DCC in accordance with Section F10.8 (Ordering, Delivery, Rejection and Returns);

(s) ('*additional CH Order Management System accounts*') the number of additional CH Order Management System accounts made available to that Party during that Charging Period in accordance with Section F5.23 (CH Order Management System Accounts);

(t) ('*shared solution Alt HAN Equipment*') the number (as measured at the end of that Charging Period) of MPANs associated with premises supplied with electricity by that Party and of MPRNs associated with premises supplied with gas by that Party, in respect of each of which premises (except where the Alt HAN Inventory records that Party as having elected to use Opted-out Alt HAN Equipment at that time) Central Shared Solution Alt HAN Equipment is installed;

(u) ('*point-to-point Alt HAN Equipment*') the number (as measured at the end of that Charging Period) of MPANs associated with premises supplied with electricity by that Party and of MPRNs associated with premises supplied with gas by that Party, in respect of each of which premises (except where the Alt HAN Inventory records that Party as having elected to use Opted-out Alt HAN Equipment at that time) Central Point-to-Point Alt HAN Equipment is installed;

(v) ('*stock level point-to-point Alt HAN Equipment*') the number of items of Central Point-to-Point Alt HAN Equipment (as measured at the end of that Charging Period) delivered to that Party but not installed;

(w) (*'RF Noise Testing'*) an obligation to pay arising during that Charging Period from the acceptance by that Party of the charges offered by the DCC to provide RF Noise Testing pursuant to Section H14.37 (Radio Frequency Noise Testing);

(x) (*'DCC Boxed'*) the number of each of the types of DCC Boxed which have been delivered to that Party during that Charging Period under Section H14 (Testing Services) and in accordance with Clause 18 of the Enduring Testing Approach Document; and

(y) (*'MAP/Manufacturer Reports'*) the number of MAP/Manufacturer reports provided to the Meter Asset Provider or Manufacturer during that Charging Period.

Explicit Charges

K7.6 The DCC will determine the Explicit Charges for each Explicit Charging Metric and each Regulatory Year:

(a) in the case of the Explicit Charging Metrics referred to in Section K7.5(a) and (b)('security assessments' and 'privacy assessments'), so as to pass-through to each Party the relevant expenditure incurred by the Panel in respect of the Explicit Charging Metric as notified by the Panel to the DCC for the purpose of establishing such Charges;

(b) (subject to Section K7.6(a)) in a manner consistent with the Charging Objectives referred to in Sections C1.4, C1.5 and C1.6(a), (b), and (c);

(c) (subject to Section K7.6(a) and the Charging Objective referred to in Section C1.4) on a non-discriminatory and cost reflective basis so as to recover the incremental cost to the DCC (including under the DCC Service Provider Contracts) associated with the occurrence of that Explicit Charging Metric (and disregarding any costs and expenses that would be incurred whether or not that Explicit Charging Metric occurred);

(d) in the case of the Explicit Charging Metrics referred to in Section K7.5(c) and (''LV gateway connection' and 'HV gateway connection'), the Explicit Charges may comprise an initial connection charge and an ongoing annual charge (which annual charge may be payable monthly or less frequently);

(e) in the case of the Explicit Charging Metrics referred to in Section K7.5(j) ('communication services'), in accordance with (c) above; save that (where the cost of implementing an Explicit Charge for one or more of the Services referred to in that Section would be disproportionate to the cost-reflective incremental cost) the Explicit Charge for those Services may be set at zero;

(f) in the case of the Explicit Charging Metrics referred to in Sections K7.5(l), (n), (o) and (p) ('CH stock level charge', 'CH auxiliary equipment', 'CH returned and redeployed', and 'CH returned not redeployed'), so as to ensure they are uniform across each month of a Regulatory Year and across each Region and do not make any distinction linked to use at Domestic Premises or Non- Domestic Premises;

(g) in the case of the Explicit Charging Metric referred to in Sections K7.5(l), (o) and (p) ('CH stock level charge', 'CH returned and redeployed' and 'CH returned not redeployed'), on the basis that there can be different charges for each HAN Variant;

(h) so that the Explicit Charging Metric referred to in Section K7.5(o) ('CH returned and redeployed') for each HAN Variant is not more than the Explicit Charging Metric for that HAN Variant referred to in Section K7.5(p) ('CH returned not redeployed');

(i) in the case of the Explicit Charging Metric referred to in Section K7.5(p) ('CH returned not redeployed'), in accordance with (c) above, for which purpose the incremental cost to DCC shall include any early termination fee payable in relation to the Communications Hub, or (if applicable) the net present value of the ongoing costs likely to be incurred by the DCC notwithstanding the fact that the Communications Hub has been removed, lost or destroyed;

(i)a in the case of the Explicit Charging Metric referred to in Sections K7.5(r) ('test comms hubs'), on the basis that there can be different charges for different types of Test Communications Hubs (including by reference to the HAN Variant to which they correspond); and

(j) in the case of the Explicit Charging Metrics referred to in Section K7.5(t), (u) and (v) ('shared solution Alt HAN Equipment', 'point-to-point Alt HAN Equipment' and 'stock level point-to-point Alt HAN Equipment), so as to pass- through to each Party the relevant costs of AltHANCo in respect of the Explicit Charging Metric as notified by AltHANCo to the DCC for the purpose of establishing such Charges.

K7.7 This Section K7.7 applies only in respect of the Explicit Charging Metrics referred to in Sections K7.5(f) and (g) ('elective service evaluation' and 'P&C support'). Where the DCC is simultaneously considering requests for an Explicit Charging Metric from two or more Parties, and where it would be advantageous to all such Parties for the DCC to do so, the DCC shall offer the Explicit Charging Metrics both conditionally on all the Parties taking up the Explicit Charging Metric and without such condition. In respect of the Explicit Charges to apply in respect of the conditional offer, the DCC shall calculate the Explicit Charges for each Party on the assumption that the other Parties accept the offers and shall accordingly apportion any common costs between the Parties on a non-discriminatory and cost-reflective basis.

Second-Comer Contributions

K7.8 This Section K7.8 applies only in respect of the Explicit Charging Metrics referred to in Sections K7.5(f) and (g) ('elective service evaluation' and 'P&C support'). Subject to Section K7.10, where:

(a) the DCC makes an offer in respect of any proposed Explicit Charging Metric to a person (the " **subsequent person**"); and

(b) prior to such offer being made to the subsequent person, another person (the "**initial contributor**") was obliged to pay Explicit Charges designed to recover any costs (the "**relevant costs**") that would otherwise (in accordance with this Charging Methodology) have been recoverable from the subsequent person,

then the DCC shall make an offer to the subsequent person that requires that subsequent person to pay by way of Explicit Charges such a contribution to the relevant costs as may be reasonable in all the circumstances.

K7.9 Subject to Section K7.10, where an offer made by the DCC that includes an element of relevant costs is accepted by the subsequent person, the DCC shall (following payment by the subsequent person) offer such rebate to the initial contributor as may be reasonable in all the circumstances.

K7.10 Sections K7.8 and K7.9 shall not apply:

(a) where the relevant costs are less than £20,000;

(b) where the relevant costs are between £20,000 and £500,000 (inclusive), and the initial contributor's offer for the Explicit Charging Metric was accepted more than 5 years before the offer to the subsequent contributor is made;

(c) where the relevant costs are more than £500,000, and the initial contributor's offer for the Explicit Charging Metric was accepted more than 10 years before the offer to the subsequent contributor is made; and/or

(d) where the initial contributor no longer exists or cannot be contacted by the DCC following reasonable enquiry.

K7.11 All references to an initial contributor in this Section K7 shall, in respect of any subsequent person, be interpreted so as to include any person that was previously a subsequent person in respect of the relevant costs in question and that paid Explicit Charges designed to recover an element of those relevant costs.

K8. DETERMINING ELECTIVE CHARGES

Introduction

K8.1 The Elective Charges for each Regulatory Year are payable in accordance with the relevant Bilateral Agreement.

K8.2 The terms and conditions of each Bilateral Agreement (including those in respect of the Elective Charges payable thereunder) are to be agreed or determined in accordance with Section H7 (Elective Communication Services) and the DCC Licence.

Determining the Elective Charges

K8.3 Where the DCC makes any offer to enter into a Bilateral Agreement in respect of an Elective Communication Service, the DCC shall offer Elective Charges in respect of each such Elective Communication Service determined by the DCC:

(a) in a manner consistent with the Charging Objectives referred to in Sections C1.6(a), (b), and (c);

(b) in a non-discriminatory and cost-reflective manner, so as to recover the total costs to the DCC (including under the DCC Service Provider Contracts) associated with that Bilateral Agreement (including so as to recover a reasonable proportion of any standing costs that would be incurred whether or not that Elective Communication Service was provided); and

(c) so that such proportion of such standing costs is recovered by way of a standing charge that is payable whether or not the service is requested or provided.

K8.4 Where the DCC is simultaneously considering requests for a formal offer to provide Elective Communication Services from two or more Parties, and where it would be advantageous to all such Parties for the DCC to do so, the DCC shall make the offer both conditionally on all the Parties accepting the offer and without such condition. In respect of the Elective Charges to apply in respect of the conditional offer, the DCC shall calculate the Elective Charges for each Party on the assumption that the other Parties accept the offers, and shall accordingly apportion any common costs between the Parties on a non-discriminatory and cost-reflective basis.

K8.5 Although this Code in no way binds the Authority it is acknowledged that any determination by the Authority of the Elective Charges in respect of a Bilateral Agreement will be undertaken as envisaged by the DCC Licence, including by reference to those matters set out in Sections K8.3 and K8.4.

Second-Comer Contributions

K8.6 Subject to Section K8.8, where:

(a) the DCC makes an offer in respect of any proposed Elective Communications Service to a person (the "**subsequent person**"); and

(b) prior to such offer being made to the subsequent person, another person (the "**initial contributor**") was obliged to pay Elective Charges designed to recover any costs (the "**relevant costs**") that would otherwise (in accordance with this Charging Methodology) have been recoverable from the subsequent person,

then the DCC shall make an offer to the subsequent person that requires that subsequent person to pay by way of Elective Charges such a contribution to the relevant costs as may be reasonable in all the circumstances.

K8.7 Subject to Section K8.8, where an offer made by the DCC that includes an element of relevant costs is accepted by the subsequent person, the DCC shall (following payment by the subsequent person) offer such rebate to the initial contributor as may be reasonable in all the circumstances.

K8.8 Sections K8.6 and K8.7 shall not apply:

(a) where the relevant costs are less than £20,000;

(b) where the relevant costs are between £20,000 and £500,000 (inclusive), and the initial contributor's offer for the Elective Communication Service was accepted more than 5 years before the offer to the subsequent contributor is made;

(c) where the relevant costs are more than £500,000, and the initial contributor's offer for the Elective Communication Service was accepted more than 10 years before the offer to the subsequent contributor is made; and/or

(d) where the initial contributor no longer exists or cannot be contacted by the DCC following reasonable enquiry.

K8.9 All references to an initial contributor in this Section K8 shall, in respect of any subsequent person, be interpreted so as to include any person that was previously a subsequent person in respect of the relevant costs in question and that paid Elective Charges designed to recover an element of those relevant costs.

K9. WITHIN-YEAR ADJUSTMENTS

Introduction

K9.1 The revenue restriction contained in the DCC Licence allows the DCC to carry forward any under or over recovery in respect of one Regulatory Year to the following Regulatory Year. Therefore, there is no absolute need for the DCC to alter the Charges part way through a Regulatory Year.

K9.2 Nevertheless, subject to compliance with Condition 19 of the DCC Licence, the DCC may alter the Charges part way through a Regulatory Year, including in one of the following two ways:

(a) where this Charging Methodology is amended and the amendment has effect part way through a Regulatory Year; or

(b) where the requirements of this Section K9 are met, by applying within-year adjustments for the matters set out in this Section K9.

Amending this Charging Methodology

K9.3 Where the Authority consents in accordance with Condition 19 of the DCC Licence, the DCC may recalculate the Charges in accordance with this Charging Methodology (including so as to take into account any modification of this Charging Methodology). In such circumstances, the references herein to a Regulatory Year shall be interpreted as meaning the remaining period of such Regulatory Year from the time at which the modified Charges in question are to apply.

Within-Year Adjustment for Bad Debt

K9.4 Where a Party fails to pay to the DCC an amount due by way of Charges such that an Event of Default has occurred, and provided the DCC has complied with its obligations under Section J (Charges) in respect of the same, the DCC may (where it reasonably considers it appropriate to do so, taking into account the matters referred to in Section K9.1) determine the **Unrecovered Bad Debt Payment** $(\mathrm{UBDP}_{\mathrm{pemt}})$ to be paid by every Compliant Party (p) in respect of that Event of Default (e) in one or more subsequent months (m) of such Regulatory Year (t) as the DCC may determine. $(\mathrm{UBDP}_{\mathrm{pemt}})$ shall be calculated as follows:

$$UBDP_{pemt} = \frac{UBP_e \times DS_{pe}}{BM_e}$$

Where:

BM_e is the number of months in the balance of the Regulatory Year over which the DCC decides it is to recover the amount owing in respect of the Event of Default

UBP_e is the amount owing in respect of the Event of Default (e) or such smaller amount as DCC decides to recover over the remainder of the Regulatory Year (t)

DS_{pe} is the share of the debt owing in respect of the Event of Default (e) to be paid by each Compliant Party (p), which is to be calculated as follows.

$$DS_{pe} = \frac{TMP_{pe}}{\sum_{\forall p} TMP_{pe}}$$

where TMP_{pe} is the total amount paid or payable by way of Charges by each Compliant Party (p) in respect of the 12 months preceding the month in respect of which the Event of Default (e) occurred

$\sum_{\forall p}$ represents a sum over all Compliant Parties for the Event of Default.

K9.5 Where the DCC:

(a) has levied a charge for an Unrecovered Bad Debt Payment; and

(b) subsequently recovers from the defaulting Party any or all of the unpaid debt to which the Unrecovered Bad Debt Payment related,

then the DCC shall return the money it has recovered from the defaulting Party to the Compliant Parties in proportion to their contributions to $UBDP_{pemt}$. In order to return such money, the DCC shall include a negative $UBDP_{pemt}$ amount in the Charges for the month following the month in which the DCC received payment (or part payment) from the defaulting Party.

Within-Year Adjustment for Liability Events

K9.6 If a Liability Event arises, the DCC may (where it reasonably considers it appropriate to do so, taking into account the matters referred to in Section K9.1 and having consulted with the Authority and the Panel) determine the **Liability Payment** (LP_{plmt}) to be paid by (or, in the case of negative Liability Sums, paid to) every other Party (p) in respect of that Liability Event (l) in one or more subsequent months (m) of such Regulatory Year (t) as the DCC may determine LP_{plmt} shall be calculated as follows:

$$LP_{plmt} = \frac{TLP_l \times LS_{pl}}{BM_l}$$

Where:

BM_l is the number of months in the balance of the Regulatory Year over which the DCC decides it is to recover the amount owing in respect of the Liability Event

TLP_l is the Liability Sum arising in respect of the Liability Event (l) or such smaller amount as DCC decides to recover over the remainder of the Regulatory Year (t)

LS_{pl} is the share of the liability owing in respect of the Liability Event (l) to be paid by (or, in the case of negative Liability Sums, paid to) each Party (p), which is to be calculated as follows.

$$LS_{pl} = \frac{TMP_{pl}}{\sum_{\forall p} TMP_{pl}}$$

where TMP_{pl} is the total amount paid or payable by way of Charges by each Party (p) in respect of the 12 months preceding the month in which the Liability Sum for the Liability Event (l) is payable to or by the DCC Service Providers $\sum_{\forall p}$ represents a sum over all Parties.

Within-Year Adjustment for Communications Hub Finance Acceleration Events

K9.7 For the purposes of Section K9.6:

(a) a Communications Hub Finance Acceleration Event and a 4G DBT Finance Acceleration Event are each a Liability Event;

(b) the amount due and payable by the DCC as a result of a Communications Hub Finance Acceleration Event and/or 4G DBT Finance Acceleration Event is a Liability Sum to the extent the DCC estimates that such amount will be recoverable by the DCC as Allowed Revenue;

(c) the reference to “Charges” in the definition of LS_{pl} shall (in the case of a Communications Hub Finance Acceleration Event) be interpreted as a reference to “Communications Hub Charges” and in the case of a 4G DBT Finance Acceleration Event be interpreted as a reference to "Fixed Charges"; and

(d) the amount payable by each Party in respect of such Liability Event shall (for the purposes of invoicing and payment under Section J (Charges) or Section M11.5(b) (Third Party Rights)) be treated as an amount due by way of Communications Hub Finance Charges relating to the Communications Hub Finance Facility in respect of which the Communications Hub Finance Acceleration Event has occurred and/or as an amount due by way of 4G DBT Finance Charges in respect of which the 4G DBT Finance Acceleration Event has occurred (as the case may be).

K10. CALCULATING MONTHLY PAYMENTS

Introduction

K10.1 The monthly payment of Charges payable by each Party shall be calculated in accordance with this Section K10, based on:

(a) the Fixed Charges determined in accordance with Section K5 or K6 (as applicable);

(b) the Fixed CH Charges determined in accordance with Section K6A;

(c) the Fixed Alt HAN Charges determined in accordance with Section K5A, K5B or K6B (as applicable);

(d) the Explicit Charges determined in accordance with Section K7;

(e) the Elective Charges determined in accordance with Section K8; and

(f) any within-year adjustments determined in accordance with Section K9.

Calculating Fixed Charges

K10.2 The Fixed Charges, Fixed CH Charges and Fixed Alt HAN Charges payable by each person in respect of any month (or part month) during a Regulatory Year shall be calculated following the end of that month based on the calculations in accordance with Section K5, K5A, K5B, K6, K6A or K6B (as applicable).

K10.3 The Fixed Charges and Fixed CH Charges are payable by the persons in each Charging Group, and the Fixed Alt HAN Charges are payable by the persons in the Alt HAN Charging Groups. The Fixed Charges and Fixed CH Charges payable by any Party that is not in a Charging Group shall be zero, and the Fixed Alt HAN Charges payable by any Party that is not in an Alt HAN Charging Group shall be zero.

Calculating Explicit Charges and Elective Charges Payments

K10.4 The Explicit Charges payable by each Party in respect of any month (or part month) during a Regulatory Year shall be calculated following the end of that month based on the Explicit Charging Metrics incurred by that Party during the Charging Period for that month.

K10.5 The Elective Charges payable by each Party in respect of any month (or part month) during a Regulatory Year shall be calculated following the end of that month based on the relevant Bilateral Agreement.

Calculating Monthly Payments (UITMR Period)

K10.6 No longer used.

K10.7 For each month (or part month) (m) during a Regulatory Year (t) during the UITMR Period, the rollout monthly payment (*RMP*) in respect of the Charges payable by each Party (p) shall be calculated as follows:

$$\begin{aligned} RMP_{pmt} = {} & \sum_{\forall g}\left(RFC_{gt} \times \left(ADSMS_{pgmt} + \sum_{\forall r} ANSMS_{pgrmt} \right)\right) \\ & + \sum_{\forall g \forall h}\left(CHC_{ght} \times \left(ADCH_{ght} + \sum_{\forall r} ANCH_{ghrt} \right)\right) \\ & + \sum_{\forall g}\left(RAHFC_{gt} \times ADSMS_{pgmt} \right) + \sum_{\forall g}\left(RAHFC_{gt} \times \sum_{\forall r} ANSMS_{pgrmt} \right) \\ & + \sum_{i=1}^{i=n}\left(EC_{it} \times ECM_{ipmt} \right) + TEP_{pmt} + \sum_{e \in m} UBDP_{pemt} + \sum_{l \in m} LP_{plmt} \end{aligned}$$

Where:

RFC_{gt} = the Fixed Charges payable in respect of months (or part months) during Regulatory Year (t) by persons in Charging Group (g) in respect of Mandated Smart Metering Systems for Domestic Premises and Enrolled = the Fixed Charges payable in respect of months (or part months) during Regulatory Year (t) by persons in Charging Group (g) in respect of Mandated Smart Metering Systems for Domestic Premises and Enrolled Smart Metering Systems for Non-Domestic Premises, calculated in accordance with Section K5;

$ADSMS_{pgmt}$ = the amount described as such in Section K5.9;

$ANSMS_{pgrmt}$ = the amount described as such in Section K5.7;

CHC_{ght} = the Fixed CH Charge payable in respect of months (or part months) during Regulatory Year (t) by persons in CH Charging Group (g), for HAN Variant (h) in respect of Smart Metering Systems for both Non- Domestic Premises and Domestic Premises;

$ANCH_{ghrt}$ = the amount described in Section K6A.6;

$ADCH_{ght}$ = the amount described in Section K6A.6;

$RAHFC_{gt}$ = the Fixed Alt HAN Charge payable in respect of months (or part months) during Regulatory Year (t) by persons in Alt HAN Charging Group (g) in respect of Mandated Smart Metering Systems for Domestic Premises and Smart Metering Systems for Non-Domestic Premises calculated in accordance with Section K5A;

EC_{it} = the Explicit Charge for an Explicit Charging Metric (i) and a Regulatory Year (t);

ECM_{ipmt} = the Explicit Charging Metrics incurred by a Party (p) during the Charging Period for that month (m) in a Regulatory Year (t);

TEP_{pmt} = the total amount payable by a Party (p) in respect of Elective Charges and a month (m) in a Regulatory Year (t);

$UBDP_{pemt}$ = the Unrecovered Bad Debt Payment in respect of a month (m) in a Regulatory Year (t) and each Event of Default (e), as calculated in accordance with Section K9;

LP_{plmt} = the Liability Payment in respect of a month (m) in a Regulatory Year (t) and each Liability Event (l), as calculated in accordance with Section K9.

Calculating Monthly Payments (COMR Period)

K10.7A For each month (or part month) (m) during a Regulatory Year (t) during the COMR Period, the rollout monthly payment (RMP) in respect of the Charges payable by each Party (p) shall be calculated as follows:

$$
\begin{aligned}
RMP_{pmt} = & \sum_{\forall g}\left(RFC_{gt} \times \left(ADSMS_{pgmt} + \sum_{\forall r} ANSMS_{pgrmt} \right)\right) \\
& + \sum_{\forall g \forall h}\left(CHC_{ght} \times \left(ADCH_{ght} + \sum_{\forall r} ANCH_{ghrt} \right)\right) \\
& + \sum_{\forall g}\left(RAHFC_{gt} \times ADSMS_{pgmt} \right) + \sum_{\forall g}\left(RAHFC_{gt} \times \sum_{\forall r} ANSMS_{pgrmt} \right) \\
& + \sum_{i=1}^{i=n}\left(EC_{it} \times ECM_{ipmt} \right) + TEP_{pmt} + \sum_{e \in m} UBDP_{pemt} + \sum_{l \in m} LP_{plmt}
\end{aligned}
$$

Where:

RFC_{gt} = the Fixed Charges payable in respect of months (or part months) during Regulatory Year (t) by persons in Charging Group (g) in respect of Mandated Smart Metering Systems for Domestic Premises and Mandated Non-Domestic Smart Metering Systems for Non-Domestic Premises, calculated in accordance with Section K5;

$ADSMS_{pgmt}$ = the amount described as such in Section K5.9;

$ANSMS_{pgrmt}$ = the amount described as such in Section K5.11;

CHC_{ght} = the Fixed CH Charge payable in respect of months (or part months) during Regulatory Year (t) by persons in CH Charging Group (g), for HAN Variant (h) in respect of Smart Metering Systems for both Non-Domestic Premises and Domestic Premises;

$ANCH_{ghrt}$ = the amount described in Section K6A.6;

$ADCH_{ght}$ = the amount described in Section K6A.6;

$RAHFC_{gt}$ = the Fixed Alt HAN Charge payable in respect of months (or part months) during Regulatory Year (t) by persons in Alt HAN Charging Group (g) in respect of Mandated Smart Metering Systems for Domestic Premises and Mandated Non-Domestic Smart Metering Systems for Non-Domestic Premises calculated in accordance with Section K5B;

EC_{it} = the Explicit Charge for an Explicit Charging Metric (i) and a Regulatory Year (t);

ECM_{ipmt} = the Explicit Charging Metrics incurred by a Party (p) during the Charging Period for that month (m) in a Regulatory Year (t);

TEP_{pmt} = the total amount payable by a Party (p) in respect of Elective Charges and a month (m) in a Regulatory Year (t);

$UBDP_{pemt}$ = the Unrecovered Bad Debt Payment in respect of a month (m) in a Regulatory Year (t) and each Event of Default (e), as calculated in accordance with Section K9;

LP_{plmt} = the Liability Payment in respect of a month (m) in a Regulatory Year (t) and each Liability Event (l), as calculated in accordance with Section K9.

Calculating Monthly Payments (Enduring)

K10.8 For each month (or part month) (m) during a Regulatory Year (t) after the COMR Period, the monthly payment (*MP*) in respect of the Charges payable by each Party (p) shall be calculated as follows:

Where:

$$
\begin{aligned}
MP_{pmt} = & \sum_{\forall g}\left(EFC_{gt} \times \left(ADSMS_{pgmt} + \sum_{\forall r} ANSMS_{pgrmt} \right)\right) \\
& + \sum_{\forall g \forall h}\left(CHC_{ght} \times \left(ADCH_{ght} + \sum_{\forall r} ANCH_{ghrt} \right)\right) \\
& + \sum_{\forall g}\left(DAHFC_{gt} \times ADSMS_{pgmt} \right) + \sum_{\forall g}\left(NAHFC_{gt} \times \sum_{\forall r} ANSMS_{pgrmt} \right) \\
& + \sum_{i=1}^{i=n}\left(EC_{it} \times ECM_{ipmt} \right) + TEP_{pmt} + \sum_{e \in m} UBDP_{pemt} + \sum_{l \in m} LP_{plmt}
\end{aligned}
$$

Where:

EFC_{gt} = the Fixed Charges payable in respect of months (or part months) during Regulatory Year (t) by persons in Charging Group (g) in respect of Enrolled Smart Metering Systems for both Non-Domestic Premises and Domestic Premises, calculated in accordance with Section K6;

$ADSMS_{pgmt}$ = the amount described as such in Section K6.7;

$ANSMS_{pgrmt}$ = the amount described as such in Section K6.7;

CHC_{ght} = the Fixed CH Charge payable in respect of months (or part months) during Regulatory Year (t) by persons in CH Charging Group (g), for HAN Variant (h) in respect of Smart Metering Systems for both Non- Domestic Premises and Domestic Premises;

$ANCH_{ghrt}$ = the amount described in Section K6A.6;

$ADCH_{ght}$ =the amount described in Section K6A.6;

$DAHCFC_{gt}$ = the Domestic Fixed Alt HAN Charge payable in respect of months (or part months) during Regulatory Year (t) by persons in Alt HAN Charging Group (g) in respect of Enrolled Smart Metering Systems for Domestic Premises calculated in accordance with Section K6B;

$NAHFC_{gt}$ = the Non-Domestic Fixed Alt HAN Charge payable in respect of months (or part months) during Regulatory Year (t) by persons in Alt HAN Charging Group (g) in respect of Enrolled Smart Metering Systems for Non-Domestic Premises calculated in accordance with Section K6B;

EC_{it} =the Explicit Charge for an Explicit Charging Metric (i) and a Regulatory Year (t);

ECM_{ipmt} = the Explicit Charging Metrics incurred by a Party (p) during the Charging Period for that month (m) in a Regulatory Year (t);

TEP_{pmt} =the total amount payable by a Party (p) in respect of Elective Charges and a month (m) in a Regulatory Year (t);

$UBDP_{pemt}$ = the Unrecovered Bad Debt Payment in respect of a month (m) in a Regulatory Year (t) and each Event of Default (e), as calculated in accordance with Section K9;

LP_{plmt}: =the Liability Payment in respect of a month (m) in a Regulatory Year (t) and each Liability Event (l), as calculated in accordance with Section K9.

K11. DEFINITIONS

K11.1 In this Charging Methodology, except where the context otherwise requires, the expressions in the left hand column below shall have the meanings given to them in the right hand column below:

Advanced Meter has the meaning given to that expression in:

a. with respect to the supply of electricity, standard licence condition 39 of the Electricity Supply Licence;
b. with respect to the supply of gas, standard licence condition 33 of the Gas Supply Licence.

Allowed Revenue has the meaning given to that expression in the revenue restriction conditions of the DCC Licence.

Alt HAN Charging Group has the meaning given to that expression in Section K3.10.

Alt HAN Charging Group Weighting Factors has the meaning given to that expression in Section K3.15.

Alt HAN Cost Domestic Allocation has the meaning given to that expression in Section K3.17.

Alt HAN Costs has the meaning given to that expression in Section Z6.1.

Alt HAN Fixed Revenue has the meaning given to that expression in Section K3.7.

Alt HAN Inventory has the meaning given to that expression in Section Z6.1.

AltHANCo has the meaning given to that expression in Section Z6.1.

Central Point-to-Point Alt HAN Equipment has the meaning given to that expression in Section Z6.1.

Central Shared Solution Alt HAN Equipment has the meaning given to that expression in Section Z6.1.

Charging Group has the meaning given to that expression in Section K3.10.

Charging Group Weighting Factor has the meaning given to that expression in Section K3.13.

Charging Period means, in respect of each month (the ‘current month’), the period from the start of the 16th day of the previous month to the end of the 15th day of the current month.

CH Charging Group has the meaning given to that expression in Section K3.9.

CH Charging Group Weighting Factor has the meaning given to that expression in Section K3.14.

COMR Period means the period, during which mass rollout of Smart Metering Systems is to be completed, which for these purposes:

a. commences immediately following the end of the UITMR Period; and
b. ends at the end of 31 March falling in the year determined for such purposes by the Secretary of State following consultation with the Authority, Parties, and the Panel.

Compliant Party means, in respect of any Event of Default giving rise to an Unrecovered Bad Debt Payment, all of the Parties other than: (a) the Defaulting Party in respect of that Event of Default; and (b) the Defaulting Party in respect of any other Event of Default giving rise to an Unrecovered Bad Debt Payment that is calculated under Section K9.4 during the same month as the Unrecovered Bad Debt Payment to which reference is first made in this definition.

Designated Premises has the meaning given to that expression in:

a. with respect to the supply of electricity, standard licence condition 1 (Definitions for standard conditions) of the Electricity Supply Licence;
b. with respect to the supply of gas, standard licence condition 1 (Definitions for standard conditions) of the Gas Supply Licence.

Elective Charges means the Charges payable in respect of Elective Communication Services.

Enrolled Smart Metering System means a Smart Metering System that has been Enrolled.

Estimated Allowed Revenue has the meaning given to that expression in Section K2.1.

Estimated Elective Service Revenue has the meaning given to that expression in Section K2.3.

Estimated Explicit Charges Revenue has the meaning given to that expression in Section K2.5.

Estimated Fixed Charges Revenue has the meaning given to that expression in Section K2.6.

Exit Criteria means the criteria that must be satisfied before testing can be considered complete.

Explicit Charges means the Charges calculated in accordance with Section K7, and payable in respect of the Explicit Charging Metrics.

Explicit Charging Metrics has the meaning given to that expression in Section K7.

Fixed Alt HAN Charges means the Charges calculated in accordance with Section K5A, K5B or K6B (as applicable).

Fixed CH Charges means the Charges calculated in accordance with Section K6A.

Fixed Charges means the Charges calculated in accordance with Section K5 or K6 (as applicable).

HAN Variant for the purposes of this Section K there shall be only two HAN Variants: Single Band and Dual Band, as further described in Appendix I (CH Installation and Maintenance Support Materials).

Liability Event means an event as a result of which either:
(a) the DCC has a net liability to the DCC Service Providers collectively (excluding in respect of charges arising in the ordinary course of events); or
(b) the DCC Service Providers collectively have a net liability to the DCC (excluding in respect of service credits or liquidated damages arising from poor service performance).

Liability Sum means, in respect of a Liability Event as a result of which:
(a) the DCC owes a net liability to the DCC Service Providers collectively, the amount of such net liability (having taken into account amounts recoverable by the DCC in respect of that Liability Event otherwise than pursuant to this Charging Methodology, including amounts recoverable from other Parties as a result of any breach of this Code by such Parties which caused or contributed to that Liability Event), but only to the extent that the DCC estimates that such net liability will be recoverable by the DCC as Allowed Revenue; or
(b) the DCC Service Providers collectively owe a net liability to the DCC, the net amount actually received by the DCC in respect of such net liability (having taken into account amounts owed by the DCC to other Parties and to third parties in respect of that Liability Event otherwise than pursuant to this Charging Methodology), but only to the extent that the DCC estimates that such net liability will reduce the Allowed Revenue that the DCC could otherwise recover by way of the Charges (which net amount will be expressed as a negative number).

Liability Payment has the meaning given to that expression in Section K9.6 (expressed as a negative number in the case of negative Liability Sums).

Mandated Non-Domestic Smart Metering System means, from time to time, each MPAN or MPRN associated with a Designated Premises (regardless of whether or not a Smart Metering System has been installed or Enrolled), but excluding:

a. those MPANs and MPRNs associated with premises in respect of which the DCC is exempted from the requirement to Enrol Smart Metering Systems in accordance with the Statement of Service Exemptions;
b. those MPANs that do not have the status of “traded” (as identified in the REC) and those MPRNs that do not have a status that indicates that gas is off-taken at the supply point (as identified in the UNC);
c. those MPANs associated with a Designated Premises at which there is installed an Advanced Meter pursuant to the provisions of standard condition 39 of the Electricity Supply Licence; and
d. those MPRNs associated with a Designated Premises at which there is installed an Advanced Meter pursuant to the provisions of standard condition 33 of the Gas Supply Licence.

Mandated Smart Metering System means, from time to time, each MPAN or MPRN associated with a Domestic Premises (regardless of whether or not a Smart Metering System has been installed or Enrolled), but excluding:

a. those MPANs and MPRNs associated with premises in respect of which the DCC is exempted from the requirement to Enrol Smart Metering Systems in accordance with the Statement of Service Exemptions; and
b. those MPANs and MPRNs that do not have an RMP Lifecycle Status of 'operational' (as recorded pursuant the REC).

National Fixed Revenue has the meaning given to that expression in Section K3.7.

Opted-out Alt HAN Equipment has the meaning given to that expression in Section Z6.1.

Regional Communications Hub Device Revenue has the meaning given to that expression in Section K3.9.

Regional Communications Hub Fixed Revenue has the meaning given to that expression in Section K3.9.

Regional Fixed Revenue has the meaning given to that expression in Section K3.9.

Regulatory Year means (subject to Section K9.3) a period of twelve months beginning at the start of 1 April in any calendar year and ending at the end of 31 March in the next following calendar year.

Test CH Services means the Services provided under Section F10 (Test Communications Hubs).

UITMR Period means the period, covering User integration testing and the mass rollout period, which for these purposes:

(a) commences at the start of the month in which the DCC is first obliged to make regular monthly payments to one or more of the DCC Service Providers;

and
(b) ends on 31 March 2021.

Unrecovered Bad Debt Payment has the meaning given to that expression in Section K9.4.

Unrecovered Bad Debt Payment has the meaning given to that expression in Section K9.4.

Weighting Factor means the Charging Group Weighting Factor, the CH Charging Group Weighting Factor or the Alt HAN Charging Group Weighting Factor.

Contents

L SMART METERING KEY INFRASTRUCTURE AND DCC KEY INFRASTRUCTURE

L1. SMKI POLICY MANAGEMENT AUTHORITY

Establishment of the SMKI PMA

L1.1 The Panel shall establish a Sub-Committee in accordance with the requirements of this Section L1, to be known as the "**SMKI PMA**".

L1.2 Save as expressly set out in this Section L1, the SMKI PMA shall be subject to the provisions concerning Sub-Committees set out in Section C6 (Sub-Committees).

Membership of the SMKI PMA

L1.3 The SMKI PMA shall be composed of the following persons (each an "**SMKI PMA Member**"):

(a) the SMKI PMA Chair (as further described in Section L1.5);

(b) four SMKI PMA (Supplier) Members (as further described in Section L1.6);

(c) two SMKI PMA (Network) Member (as further described in Section L1.8); and

(d) one representative of the Security Sub-Committee and one representative of the Technical Architecture and Business Architecture Sub-Committee (in each case as further described in Section L1.10); and

(e) one SMKI Specialist (appointed as described in the definition of that expression in Section A1 (Definitions)).

L1.4 Each SMKI PMA Member must be an individual (and cannot be a body corporate, association or partnership). No one person can hold more than one office as an SMKI PMA Member at the same time.

L1.5 The "**SMKI PMA Chair**" shall be such person as is (from time to time) appointed to that role by the Panel in accordance with a process designed to ensure that:

(a) the candidate selected is sufficiently independent of any particular Party or class of Parties;

(b) the SMKI PMA Chair is appointed for a three-year term (following which he or she can apply to be re-appointed);

(c) the SMKI PMA Chair is remunerated at a reasonable rate;

(d) the SMKI PMA Chair's appointment is subject to Section C6.9 (Member Confirmation), and to terms equivalent to Section C4.6 (Removal of Elected Members);

(e) provision is made for the SMKI PMA Chair to continue in office for a reasonable period following the end of his or her term of office in the event of any delay in appointing his or her successor; and

(f) where the SMKI PMA Chair's appointment (and for the purposes of this Section and Section L1.5A all references to appointment shall encompass re-appointment) is to take effect on or after the date this Section L1.5(f) comes into force, the Panel shall:

(i) notify the Secretary of State of the appointment it proposes to make;

(ii) not make the appointment unless and until the Secretary of State has confirmed in writing that they do not object to the appointment being made;

(iii) ensure that the terms of the appointment include terms which provide for the Panel to terminate the appointment where directed to do so by the Secretary of State pursuant to Section L1.5A and from such date or within such period as may be specified in the Secretary of State's direction; and

(iv) where the appointed person has not, at the date of the appointment, passed (as a minimum) a Security Check (or equivalent), ensure that the terms of the appointment include terms which:

(A) require the appointed person to apply for a Security Check (or equivalent) within one month of the date of the appointment;

(B) provide for the Panel to terminate the appointment if a Security Check (or equivalent) is not passed by the appointed person within 12 months of the date of the appointment (or such longer period as the Secretary of State may approve following a request from the Panel).

L1.5A The Secretary of State may, in respect of any SMKI PMA Chair appointment which takes effect on or after the date Section L1.5(f) comes into force, direct the Panel to terminate the appointment of the SMKI PMA Chair where the Secretary of State considers it necessary to do for the purposes of preserving the integrity of, and in the interests of maintaining, the security of the End-to-End Smart Metering System (or any part of that system).

L1.5B The Panel shall comply with any direction given to it by the Secretary of State pursuant to Section L1.5A.

L1.6 Each of the four "**SMKI PMA (Supplier) Members**" shall (subject to any directions to the contrary made by the Secretary of State for the purpose of transition on the incorporation of this Section L1 into this Code):

(a) be appointed in accordance with Section L1.7, subject to compliance by the appointed person with Section C6.9 (Member Confirmation);

(b) retire 2 years after his or her appointment (without prejudice to his or her ability to be nominated for a further term of office); and

(c) be capable of being removed from office in accordance with Sections C4.5 and C4.6 (Removal of Elected Members), for which purpose those Sections shall be read as if references to "Elected Member" were to "SMKI PMA (Supplier) Member", references to "Panel" were to "SMKI PMA", references to "Panel Chair" were to "SMKI PMA Chair", and references to "Panel Members" were to "SMKI PMA Members".

L1.7 Each of the four SMKI PMA (Supplier) Members shall be appointed in accordance with a process:

(a) by which three SMKI PMA (Supplier) Members will be elected by Large Supplier Parties, and one SMKI PMA (Supplier) Member will be elected by Small Supplier Parties;

(b) by which any person (whether or not a Supplier Party) shall be entitled to nominate candidates to be elected as an SMKI PMA (Supplier) Member; and

(c) that is otherwise the same as that by which Elected Members are elected under Sections C4.2 and C4.3 (as if references therein to "Panel" were to "SMKI PMA", references to "Panel Chair" were to "SMKI PMA Chair", references to "Panel Members" were to "SMKI PMA Members", and references to provisions of Section C or D were to the corresponding provisions set out in or applied pursuant to this Section L1).

L1.8 The two "**SMKI PMA (Network) Members**" shall (subject to any directions to the contrary made by the Secretary of State for the purpose of transition on the incorporation of this Section L1 into this Code):

(a) be appointed in accordance with Section L1.9, subject to compliance by the appointed person with Section C6.9 (Member Confirmation);

(b) retire 2 years after his or her appointment (without prejudice to his or her ability to be nominated for a further term of office); and

(c) be capable of being removed from office in accordance with Sections C4.5 and C4.6 (Removal of Elected Members), for which purpose those Sections shall be read as if references to "Elected Member" were to "SMKI PMA (Network) Members", references to "Panel" were to "SMKI PMA", references to "Panel Chair" were to "SMKI PMA Chair", and references to "Panel Members" were to "SMKI PMA Members".

L1.9 The two SMKI PMA (Network) Member shall be appointed in accordance with a process:

(a) by which one SMKI PMA (Network) Member will be elected by the Electricity Network Parties and one SMKI PMA (Network) Member will be elected by the Gas Network Parties; and

(b) that is otherwise the same as that by which Elected Members are elected under Sections C4.2 and C4.3 (as if references therein to "Panel" were to "SMKI PMA", to "Panel Chair" were to "PMA Chair", to "Panel Members" were to "SMKI PMA Members", and to provisions of Section C or D were to the corresponding provisions set out in or applied pursuant to this Section L1).

L1.10 The Security Sub-Committee and the Technical Architecture and Business Architecture Sub-Committee shall each nominate one of their members to be an SMKI PMA Member by notice to the Secretariat from time to time. The Security Sub-Committee or the Technical Architecture and Business Architecture Sub-Committee (as applicable) may each replace its nominee from time to time by prior notice to the Secretariat. Such nomination or replacement shall be subject to compliance by the relevant person with Section C6.9 (Member Confirmation). Until each such Sub-Committee exists, the Panel shall nominate a person to act as a representative of that Sub-Committee (and may from time to time replace such person).

L1.11 Each SMKI PMA Member must ensure that he or she reads the SMKI Document Set when first appointed, and subsequently from time to time, so that he or she is familiar with its content.

Proceedings of the SMKI PMA

L1.12 Each SMKI PMA Member shall be entitled to appoint an Alternate in accordance with Section C5.19 (as it applies pursuant to Section L1.15). The SMKI PMA Chair must nominate another person to act as Alternate for the SMKI PMA Chair (which person may be the SMKI Specialist but may not be another SMKI PMA Member, and which person must be sufficiently independent of any particular Party or class of Parties).

L1.13 No business shall be transacted at any meeting of the SMKI PMA unless a quorum is present at that meeting. The quorum for each such meeting shall be four of the SMKI PMA Members, at least one of whom must be the SMKI PMA Chair (or his or her Alternate).

L1.14 Without prejudice to the generality of Section C5.13(c) (Attendance by Other Persons) as it applies pursuant to Section L1.15:

(a) a representative of the DCC shall be invited to attend each and every SMKI PMA meeting (which representative shall be entitled to speak at SMKI PMA meetings without the permission of the SMKI PMA Chair); and

(b) other persons who may be invited to attend SMKI PMA meetings may include:

(i) the Independent SMKI Assurance Service Provider;

(ii) one or more representatives of Device Manufacturers; or

(iii) a specialist legal adviser.

L1.15 Subject to Sections L1.12, L1.13 and L1.14, the provisions of Section C5 (Proceedings of the Panel) shall apply to the proceedings of the SMKI PMA, for which purpose that Section shall be read as if references to "Panel" were to "SMKI PMA", references to "Panel Chair" were to "SMKI PMA Chair", and references to "Panel Members" were to "SMKI PMA Members".

L1.16 Notwithstanding Section C3.12 (Protections for Panel Members and Others), that Section shall not apply to the SMKI Specialist in any circumstances and the SMKI Specialist shall have no rights under that Section.

Duties of the SMKI PMA

L1.17 The SMKI PMA shall undertake the following duties:

(a) to approve the Device CPS, Organisation CPS and the IKI CPS, and any changes to those documents, in accordance with Sections L9;

(b) to propose variations to the SMKI SEC Documents, as further described in Section L1.19;

(c) to periodically review (including where directed to do so by the Panel) the effectiveness of the SMKI Document Set (including so as to evaluate whether the SMKI Document Set remains consistent with the SEC Objectives), and report to the Panel on the outcome of such review (such report to include any recommendations for action that the SMKI PMA considers appropriate);

(d) as soon as reasonably practicable following the incorporation of each of the following documents into this Code, its re-incorporation, or its modification in accordance with section 88 of the Energy Act 2008, to review that document in accordance with paragraph (c) above:

(i) the SMKI Compliance Policy;

(ii) the SMKI RAPP;

(iii) the Device Certificate Policy;

(iv) the Organisation Certificate Policy;

(v) the IKI Certificate Policy;

(vi) the SMKI Recovery Procedure,

and (where the SMKI PMA considers it appropriate to do so) submit one or more Draft Proposals in respect of those documents;

(e) to periodically review the effectiveness of the DCCKI Document Set and to:

(i) notify DCC where it considers that changes should be made to the DCCKI Document Set in order to ensure that DCC meets its obligations under Section G (Security) (such notification to include any recommendation for action that the SMKI PMA considers appropriate); and

(ii) copy any such notification to the Security Sub-Committee and, except to the extent that it is appropriate to redact information for security purposes, to other SEC Parties;

(f) as soon as reasonably practicable following the incorporation of each of the following documents into this Code, its re-incorporation, or its modification in accordance with section 88 of the Energy Act 2008, to review that document in accordance with paragraph (e) above:

(i) the DCCKI RAPP;

(ii) the DCCKI Certificate Policy;

(g) to review the DCCKI CPS, and any amendments proposed to be made to it by the DCC, in accordance with Section L13 (DCC Key Infrastructure);

(h) as part of its review of the SMKI Compliance Policy pursuant to paragraph (d) above, to consider whether SMKI Participants which are subject to assurance assessments pursuant to the SMKI Compliance Policy should be liable to meet the costs (or a proportion of the costs) of undertaking such assessments, and (where the SMKI PMA considers it appropriate to do so) submit one or more Draft Proposals as referred to in paragraph (d) above;

(i) in relation to any incident in which a Relevant Private Key is (or is suspected of being) Compromised, to decide, in accordance with the SMKI Recovery Key Guidance, whether or not to require the use of the Recovery Private Key or Contingency Private Key (including in the latter case the use of the Contingency Symmetric Key);

(j) to exercise the functions allocated to it under the SMKI Recovery Procedure, and in particular to exercise any power to nominate Parties for such purposes (and in accordance with such procedures) as may be set out in the SMKI Recovery Procedure;

(k) to provide the Panel, the Change Sub-Committee, the Change Board and Working Groups with support and advice in respect of Draft Proposals and Modification Proposals that provide for variations to the SMKI SEC Documents, the DCCKI SEC Documents, or the S1SPKM SEC Documents;

(l) to provide assurance in accordance with Section L2 (SMKI Assurance);

(m) to provide the Panel with support and advice in respect of Disputes for which the Panel is required to make a determination, insofar as such Disputes relate to the SMKI Document Set, the DCCKI Document Set or the S1SPKM Document Set;

(n) to provide the Panel and Sub-Committees with general advice and support with respect to the SMKI Services, the SMKI Repository Service, the DCCKI Services, the DCCKI Repository Service, each S1SPKI and each SMETS1 Symmetric Key Arrangement;

(o) to exercise such functions as are allocated to it under, and to comply with all the applicable requirements of, the SMKI Document Set in accordance with Section L9.1;

(p) in respect of each S1SPKI CPS, to review, and either to approve or determine not to reject (subject to such amendments as it may direct), or to reject:

(i) a draft of that document, in accordance with Section L14.11;

(ii) any proposed amendment to that document, in accordance with Section L14.13;

(q) to periodically review the effectiveness of the S1SPKM Document Set and to:

(i) notify DCC where it considers that changes should be made to the S1SPKM Document Set (such notification to include any recommendation for action that the SMKI PMA considers appropriate); and

(ii) copy any such notification to the Security Sub-Committee;

(r) as soon as reasonably practicable following the incorporation of each of the following documents into this Code, its re-incorporation, or its modification in accordance with section 88 of the Energy Act 2008, to review that document in accordance with paragraph (q) above:

(i) each S1SPKI Certificate Policy;

(ii) each S1SPKI RAPP;

(iii) each SMETS1 Cryptographic Key Management Policy;

(iv) the S1SPKM Compliance Policy; and

(s) to perform any other duties expressly ascribed to the SMKI PMA elsewhere in this Code.

L1.18 The SMKI PMA shall establish a process whereby the Code Administrator monitors Draft Proposals and Modification Proposals with a view to identifying (and bringing to the SMKI PMA's attention) those proposals that are likely to affect the SMKI SEC Documents. The Code Administrator shall comply with such process.

Modification of the SMKI SEC Documents and S1SPKM SEC Documents by the SMKI PMA

L1.19 Notwithstanding Section D1.3 (Persons Entitled to Submit Draft Proposals):

(a) the SMKI PMA shall be entitled to submit Draft Proposals in respect of any of the SMKI SEC Documents or S1SPKM SEC Documents where the SMKI PMA considers it appropriate to do so; and

(b) any SMKI PMA Member shall be entitled to submit Draft Proposals in respect of any of the SMKI SEC Documents or S1SPKM SEC Documents where he or she considers it appropriate to do so (where the SMKI PMA has voted not to do so).

Updated or Replacement Standards, Procedures and Guidelines

L1.20 In respect of the SMKI Document Set, the SMKI Services, the DCCKI Document Set, the DCCKI Services and Sections L2 to L13 shall be interpreted in accordance with the following provisions of this Section L1.

L1.21 As a consequence of its duties under Section L1.17, the SMKI PMA shall determine any updates that are required to standards, procedures and guidelines that apply to the operation of the SMKI Services and the DCCKI Services and shall publish the latest versions on the Website.

Transitional Period for Updated or Replacement Standards, Procedures and Guidelines

L1.22 Section L1.23 applies where:

(a) the DCC or any User is required, in accordance with any provision of the SMKI SEC Documents, to ensure that it, or that any of its policies, procedures, systems or processes, complies with:

(i) any standard, procedure or guideline issued by a third party; and

(ii) any equivalent to that standard, procedure or guideline which updates or replaces it from time to time; and

(b) the relevant third party issues an equivalent to that standard, procedure or guideline which updates or replaces it.

L1.23 Where this Section L1.23 applies, the obligation on the DCC or User (as the case may be):

(a) shall be read as an obligation to comply with the updated or replaced standard, procedure or guideline from such date as is determined by the SMKI PMA in respect of that document; and

(b) prior to that date shall be read as an obligation to comply (at its discretion) with either:

(i) the previous version of the standard, procedure or guideline; or

(ii) the updated or replaced standard, procedure or guideline.

L1.24 Any date determined by the SMKI PMA in accordance with Section L1.23 may be the subject of an appeal by the DCC or any User to the Panel (whose decision shall be final and binding for the purposes of this Code).

L2. SMKI ASSURANCE

SMKI Compliance Policy

L2.1 The SMKI PMA shall exercise the functions allocated to it by the SMKI Compliance Policy.

L2.2 The DCC shall procure all such services as are required for the purposes of complying with its obligations under the SMKI Compliance Policy.

SMKI Participants: Duty to Cooperate in Assessment

L2.3 Each SMKI Participant shall do all such things as may be reasonably requested by the SMKI PMA, or by any person acting on behalf of or at the request of the SMKI PMA (including in particular the Independent SMKI Assurance Service Provider), for the purposes of facilitating an assessment of that SMKI Participant's compliance with any applicable requirements of the SMKI Document Set.

L2.4 For the purposes of Section L2.3, an SMKI Participant shall provide the SMKI PMA (or the relevant person acting on its behalf or at its request) with:

(a) all such Data as may reasonably be requested, within such times and in such format as may reasonably be specified; and

(b) all such other forms of cooperation as may reasonably be requested, including in particular access at all reasonable times to:

(i) such parts of the premises of that SMKI Participant as are used for; and

(ii) such persons engaged by that SMKI Participant as carry out, or are authorised to carry out,

any activities related to its compliance with the applicable requirements of the SMKI Document Set.

Events of Default

L2.5 In relation to an Event of Default which consists of a material breach by an SMKI Participant of any applicable requirements of the SMKI Document Set, the provisions of Sections M8.2 (Notification of an Event of Default) to M8.4 (Consequences of an Event of Default) shall apply subject to the provisions of Sections L2.6 to L2.13.

L2.6 For the purposes of Sections M8.2 to M8.4 as they apply pursuant to Section L2.5, an Event of Default shall (notwithstanding the ordinary definition thereof) be deemed to have occurred in respect of the DCC where it is in material breach of any applicable requirements of the SMKI Document Set (provided that Sections M8.4(e), (f) and (g) shall never apply to the DCC).

L2.7 Where in accordance with Section M8.2 the Panel receives notification that an SMKI Participant is in material breach of any applicable requirements of the SMKI Document Set, it shall refer the matter to the SMKI PMA. On any such referral, the SMKI PMA may investigate the matter in accordance with Section M8.3 as if the references in that Section to the “Panel” were to the “SMKI PMA”.

L2.8 Where the SMKI PMA has:

(a) carried out an investigation in accordance with Section M8.3; or

(b) received a report from the Independent SMKI Assurance Service Provider, following an assessment by it of the compliance of any SMKI Participant with the applicable requirements of the SMKI Document Set, concluding that the SMKI Participant has not complied with those requirements,

the SMKI PMA shall consider the information available to it and shall determine whether any non-compliance with the SMKI Document Set has occurred and, if so, whether that non-compliance constitutes an Event of Default.

L2.9 Where the SMKI PMA determines that an Event of Default has occurred, it shall:

(a) notify the relevant SMKI Participant and any other Party it considers may have been affected by the Event of Default; and

(b) refer the matter to the Panel for the Panel to determine the appropriate steps to take in accordance with Section M8.4.

L2.10 Where the Panel is considering what steps to take in accordance with Section M8.4, it shall request and consider the advice of the SMKI PMA.

L2.11 Where the Panel determines that an SMKI Participant is required to give effect to a remedial action plan in accordance with Section M8.4(d) that plan must be approved by the SMKI PMA.

L2.12 Where, in accordance with Section L2.11, the SMKI PMA has approved a remedial action plan in relation to the provision by the DCC of the SMKI Services, the Panel shall ensure that the approved plan (being redacted only in so far as necessary for the purposes of security) is made available to all Parties.

L2.13 Where, in accordance with Section L2.11, the SMKI PMA has approved a remedial action plan in relation to:

(a) the DCC acting in a capacity other than as the provider of the SMKI Services, the Panel may arrange for a version of the approved plan (or parts of that plan) to be made available to all the Parties; or

(b) any other SMKI Participant, the Panel may arrange for an anonymised version of the approved plan (or parts of that plan) to be made available to all the Parties,

but (in each case) only where the Panel considers that such dissemination is necessary for the purposes of security.

Emergency Suspension of SMKI Services

L2.14 Where the SMKI PMA has reason to believe that there is any immediate threat of the DCC Total System, any User Systems, any Smart Metering Systems or any RDP Systems being Compromised to a material extent by the occurrence of an event arising in relation to the SMKI Services, it may instruct the DCC immediately to suspend:

(a) the provision (in whole or in part) of the SMKI Services and/or any other Services which rely on the use of Certificates;

(b) the rights of any SMKI Participant to receive (in whole or in part) the SMKI Services and/or any other Services which rely on the use of Certificates,

and thereafter to retain that suspension in effect until such time as the SMKI PMA instructs the DCC to reinstate the provision of the relevant Services or the rights of the SMKI Participant (as the case may be).

L2.15 Where the SMKI PMA takes any steps under Section L2.14, it:

(a) shall immediately thereafter notify the Authority;

(b) shall comply with any direction given to it by the Authority in relation to such steps; and

(c) may notify all the Parties of some or all of such steps (without identifying the SMKI Participant), but only where the Panel considers that such notification is necessary for the purposes of security.

L2.16 Any Party which is affected by the SMKI PMA taking any steps under Section L2.14 may appeal the decision to do so to the Authority, and the DCC shall comply with any decision of the Authority in respect of the matter (which shall be final and binding for the purposes of this Code).

L3. THE SMKI SERVICES

The SMKI Services

L3.1 For the purposes of this Section L3, the "**SMKI Services**" means all of the activities undertaken by the DCC in its capacity as:

(a) the Device Certification Authority;

(b) the Organisation Certification Authority; or

(c) the IKI Certification Authority,

in each case in accordance with the applicable requirements of the Code.

Authorised Subscribers

General Provisions

L3.2 For the purposes of this Section L3:

(a) any Party which has successfully completed the SMKI and Repository Entry Process Tests for the purposes of Section H14.22(a) in respect of any of the Certificate Policies;

(b) any RDP which has successfully completed the SMKI and Repository Entry Process Tests for the purposes of Section H14.22(a) in respect of the Organisation Certificate Policy; and

(c) SECCo or a Manufacturer in respect of the IKI Certificate Policy,

may apply to become an Authorised Subscriber in accordance with, and by following the relevant procedures set out in, that Certificate Policy and the SMKI RAPP.

L3.3 The DCC shall authorise SECCo, any Party, a Manufacturer or any RDP to submit a Certificate Signing Request, and so to become an Authorised Subscriber, where SECCo, that Party, that Manufacturer or that RDP has successfully completed the relevant procedures and satisfied the criteria set out in the relevant Certificate Policy and the SMKI RAPP.

L3.4 The DCC shall provide any SMKI Services that may be requested by an Authorised Subscriber where the request is made by that Authorised Subscriber in accordance with the applicable requirements of the SMKI SEC Documents.

L3.5 The DCC shall ensure that in the provision of the SMKI Services it acts in accordance with Good Industry Practice.

Registration Data Providers

L3.6 Where a Registration Data Provider (other than an Electricity Network Party or Gas Network Party which is deemed to be an RDP, acting in its capacity as such) has become an Authorised Subscriber, the

Network Party that nominated that Registration Data Provider shall ensure that the RDP complies with all of its obligations in that capacity under this Section L.

L3.7 Where a Registration Data Provider has been nominated as such by more than one Network Party:

(a) that RDP shall not, by virtue of acting in the capacity of an RDP for different Network Parties, be required to become a Subscriber for different Organisation Certificates;

(b) to the extent to which that RDP can be clearly identified as acting on behalf of one Network Party, that Network Party shall be subject to the requirements of Section L3.6 in respect of the actions of the RDP;

(c) to the extent to which that RDP cannot be clearly identified as acting on behalf of one Network Party, each of the Network Parties which nominated that RDP shall be subject to the requirements of Section L3.6 in respect of the actions of the RDP.

Determinations by the Panel

L3.8 Where the DCC has notified SECCo, a Party, a Manufacturer or an RDP that has applied to become an Authorised Subscriber that the DCC does not consider that it has satisfied the criteria set out in the relevant Certificate Policy and the SMKI RAPP for that purpose, SECCo, that Party, that Manufacturer or that RDP (as the case may be) may refer the matter to the Panel for determination.

L3.9 Following any reference made to it under Section L3.8, the Panel:

(a) shall determine whether the relevant applicant satisfies the criteria set out in the relevant Certificate Policy and the SMKI RAPP; and

(b) where the Panel determines that the relevant applicant meets those criteria, it shall notify the DCC, and the applicant shall (subject to any other requirements of the relevant Certificate Policy or the SMKI RAPP) become an Authorised Subscriber.

L3.10 Subject to the provisions of Section L3.11, any such determination of the Panel shall be final and binding.

L3.11 Nothing in Sections L3.8 to L3.10 shall be taken to prevent SECCo, any Party, any Manufacturer or any RDP from making a new application to DCC to become an Authorised Subscriber, in accordance with Section L3.2, at any time.

Changes in Circumstance

L3.12 Where SECCo, a Party, a Manufacturer or an RDP which is an Authorised Subscriber becomes aware of a change in circumstance which would be likely, if it were to make a new application to the DCC to become an Authorised Subscriber, to affect whether it would satisfy the criteria set out in the relevant Certificate Policy and the SMKI RAPP for that purpose, it shall as soon as is reasonably practicable notify the DCC of that change in circumstance.

L3.13 Where the DCC receives a notification from an Authorised Subscriber in accordance with Section L3.12, or otherwise becomes aware of a change in circumstance of the nature referred to in that Section, it shall:

(a) assess whether that Authorised Subscriber continues to satisfy the relevant criteria to be an Authorised Subscriber as set out in the relevant Certificate Policy and the SMKI RAPP; and

(b) where it determines that the Authorised Subscriber does not continue to satisfy the relevant criteria, notify the Authorised Subscriber which, subject to Section L3.14, shall cease to be an Authorised Subscriber in accordance with the Certificate Policy.

L3.14 Where the DCC has notified an Authorised Subscriber in accordance with Section L3.13(b):

(a) the provisions of Section L3.8 to L3.11 shall apply as if the person notified had made an unsuccessful application to become an Authorised Subscriber in respect of the relevant Certificate Policy; and

(b) where the relevant Certificate Policy is the Organisation Certificate Policy, the DCC shall, subject to any determination made by the Panel in accordance with Section L3.9, revoke any Organisation Certificates for which that person is the Subscriber;

(c) where the relevant Certificate Policy is the IKI Certificate Policy, the DCC shall, subject to any determination made by the Panel in accordance with Section L3.9, take such steps in relation to any IKI Certificates for which that person is the Subscriber as may be set out in that Certificate Policy or in the SMKI RAPP.

Eligible Subscribers

L3.15 An Authorised Subscriber:

(a) shall be known as an "**Eligible Subscriber**" in respect of a Certificate if it is entitled to become a Subscriber for that Certificate; and

(b) will be entitled to become a Subscriber for a Certificate only if it is identified as an Eligible Subscriber in respect of that Certificate in accordance with the following provisions of this Section L3.

Device Certificates

L3.16 A Party which is an Authorised Subscriber in accordance with the Device Certificate Policy will be an Eligible Subscriber in respect of a Device Certificate only where that Subject of that Device Certificate is one that is identified with that Party in the table immediately below.

Party	Subject
The DCC	Either: (a) a Communications Hub Function; or (b) a Gas Proxy Function.
An Import Supplier	Either: (a) an Electricity Smart Meter; or (b) a Type 1 Device.
A Gas Supplier	Either: (a) a Gas Smart Meter; (b) a Gas Proxy Function; or (c) a Type 1 Device.

Any other Party	Either: (a) an Electricity Smart Meter (b) a Gas Smart Meter; or (c) a Type 1 Device, but only in so far as the SMI Status of that Device is not set to 'commissioned' or 'installed not commissioned'.
The DCC acting as the Production Proving Function	Any Production Proving Device.

DCA Certificates

L3.17 Where the DCC (acting in its capacity as Root DCA or Issuing DCA) is an Authorised Subscriber in accordance with the Device Certificate Policy:

(a) it (and only it) will be an Eligible Subscriber in respect of DCA Certificates;

(b) (save for the purposes of the replacement of the Root DCA Certificate) it will be an Eligible Subscriber only in respect of a single Root DCA Certificate.

Organisation Certificates and OCA Certificates

L3.18 Where the DCC, a Network Party or another Party which is (or is to become) a User, or any RDP, is an Authorised Subscriber in accordance with the Organisation Certificate Policy, that person will be an Eligible Subscriber in respect of an Organisation Certificate or OCA Certificate only where:

(a) if the Subject of that Certificate is:

(i) either the DCC (acting pursuant to its powers or duties under the Code) or a DCC Service Provider, that person is the DCC; or

(ii) not the DCC, that person is the Subject of the Certificate; and

(b) if the value of the X520OrganizationalUnitName field in that Certificate is a Remote Party Role corresponding to that listed in the table immediately below, either:

(i) that person is the DCC, it is the Party identified with that Remote Party Role in the second column of that table, the Certificate Signing Request originates from the individual System referred in the paragraph of the definition of DCC Live Systems identified in the fourth column of that table, and the Certificate is to be issued to the same individual System from which the Certificate Signing Request originates; or

(ii) that person is identified with that Remote Party Role in the second column of that table, and the value of the subjectUniqueID field in the Certificate is a User ID or RDP ID associated with any such User Role or with an RDP as may be identified in the third column of that table.

Remote Party Role	Party	User Role or RDP	DCC Live Systems definition paragraph
root	The DCC	[Not applicable]	(d)

recovery	The DCC	[Not applicable]	(f)
transitionalCoS	The DCC	[Not applicable]	(c)
wanProvider	The DCC	[Not applicable]	(a)
accessControlBroker	The DCC	[Not applicable]	(a) or (b) (as provided for in Section L3.18A)
issuingAuthority	The DCC	[Not applicable]	(d)
networkOperator	A Network Party	Either: (a) Electricity Distributor; or (b) Gas Transporter.	[Not applicable]
supplier	A Supplier Party	Either: (a) Import Supplier; or (b) Gas Supplier.	[Not applicable]
other	An RDP or any Party other than the DCC	Either: Other User; Registered Supplier Agent; Registration Data Provider; or Export Supplier.	[Not applicable]
pPPXmlSign	The DCC	[Not Applicable]	(g)
pPRDPFileSign	The DCC	[Not Applicable]	(g)
s1SPxmlSigning	The DCC	[Not Applicable]	(h)

xmlSign	An RDP or any Party other than the DCC	Either:
		Import Supplier;
		Gas Supplier;
		Electricity Distributor;
		Gas Transporter;
		Other User;
		Registered Supplier Agent;
		Registration Data Provider; or
		Export Supplier.
			[Not applicable]

commissioningPartyFileSigning	The DCC	[Not Applicable]	[Only relevant during SMETS1 Migration]
requestingPartyFileSigning	The DCC	[Not Applicable]	[Only relevant during SMETS1 Migration]
s1SPMigrationSigning	The DCC	[Not Applicable]	[Only relevant during SMETS1 Migration]
commissioningPartyXmlSigning	The DCC	[Not Applicable]	[Only relevant during SMETS1 Migration]

loadController	None	None	[Not applicable]
cSSProvider	The DCC	[Not Applicable]	(j)
coSPartyXmlSign	The DCC	[Not Applicable]	(c)
dSPXmlSign	The DCC	[Not Applicable]	(a)
aCBXmlSign	The DCC	[Not Applicable]	(b)
wANProviderXmlSign	The DCC	[Not Applicable]	(a)

L3.18A For the purposes of the fourth column of row 5 of the above table, where:

(a) the Certificate to be issued is to have a keyUsage value of digitalSignature, the Certificate Signing Request must only have originated from the individual System referred to at paragraph (a) of the definition of DCC Live Systems; and

(b) the Certificate to be issued is to have a keyUsage value of keyAgreement, the Certificate Signing Request must only have originated from the individual System referred to at paragraph (b) of the definition of DCC Live Systems.

L3.18B For the purposes of Section L3.18A, the term 'keyUsage', 'digitalSignature', and 'keyAgreement' shall have the meaning given to that term in the Organisation Certificate Policy.

OCA Certificates (further provisions)

L3.19 Where the DCC (acting in its capacity as Root OCA or Issuing OCA) is an Authorised Subscriber in accordance with the Organisation Certificate Policy:

(a) it (and only it) will be an Eligible Subscriber in respect of OCA Certificates;

(b) (save for the purposes of the replacement of the Root OCA Certificate) it will be an Eligible Subscriber only in respect of a single Root OCA Certificate.

IKI Certificates

L3.20 Where SECCo or any Party or Manufacturer or RDP is an Authorised Subscriber in accordance with the IKI Certificate Policy, it will be an Eligible Subscriber in respect of an IKI Certificate in the circumstances set out in the IKI Certificate Policy.

ICA Certificates

L3.21 Where the DCC (acting in its capacity as Root ICA or Issuing ICA) is an Authorised Subscriber in accordance with the IKI Certificate Policy:

(a) it (and only it) will be an Eligible Subscriber in respect of ICA Certificates;

(b) (save for the purposes of the replacement of the Root ICA Certificate) it will be an Eligible Subscriber only in respect of a single Root ICA Certificate.

Certificates for Commissioning of Devices

L3.22 The DCC shall establish and lodge in the SMKI Repository, and maintain such of its Certificates as are necessary to facilitate the installation at premises of Devices that are capable of being Commissioned.

L3.23 For the purposes of Section L3.22, the DCC shall ensure that the Certificates which are established, lodged in the SMKI Repository and subsequently maintained include at least the following:

(a) the Root OCA Certificate;

(b) the Issuing OCA Certificate;

(c) the Root DCA Certificate;

(d) the Issuing DCA Certificate;

(e) the Recovery Certificate;

(f) the DCC (access-Control-Broker) - digitalSignature Certificate;

(g) the DCC (access-Control-Broker) – keyAgreement Certificate;

(h) the DCC (wanProvider) Certificate; and

(i) the DCC (transitionalCoS) Certificate.

L3.24 For the purposes of Sections L3.23(e) - (i), the Certificates which are referred to in those paragraphs mean Organisation Certificates in respect of which, in each case:

(a) the value of the KeyUsage field is that identified in relation to the Certificate in the second column of the table immediately below;

(b) the value of the X520OrganizationalUnitName field corresponds to the Remote Party Role identified in relation to the Certificate in the third column of that table; and

(c) the Certificate is used for the purposes of discharging the obligations of the DCC in the role identified in relation to it in the fourth column of that table.

Certificate	keyUsage Value	Remote Party Role	DCC Role
Recovery Certificate	digitalSignature	recovery	The role of the DCC under the SMKI Recovery Procedure.
DCC (Access Control Broker) - digitalSignature Certificate	digitalSignature	accessControlBroker	AccessControlBroker
DCC (Access Control Broker) – keyAgreement Certificate	keyAgreement	accessControlBroker	AccessControlBroker

DCC (wanProvider) Certificate	digitalSignature	wanProvider	wanProvider
DCC (transitionalCoS) Certificate	digitalSignature	transitionalCoS	The role of the DCC as CoS Party

Market Participant Identifiers

Certificate Signing Requests

L3.25 Where the DCC (acting in its capacity as Registration Authority under the Organisation Certificate Policy) receives a Certificate Signing Request of the type described in Section L3.26(a), and the circumstances described in Section L3.26(b) apply, the DCC shall reject the Certificate Signing Request.

L3.26 For the purposes of Section L3.25:

(a) a Certificate Signing Request is of the type described in this sub-paragraph (a) if it is:

(i) made by a Supplier Party;

(ii) in respect of an Organisation Certificate having a keyUsage value of digitalSignature; and

(iii) of a type that, if approved, would result in the Issue of an Organisation Certificate containing one or more Market Participant Identifiers;

(b) the circumstances described in this sub-paragraph (b) are that, at the time at which the Certificate Signing Request referred to in Section L3.25 is made:

(i) an Organisation Certificate has already been Issued by the DCC (acting in its capacity as Issuing OCA) to a Supplier Party other than the Party making the Certificate Signing Request;

(ii) that Organisation Certificate contains at least one Market Participant Identifier that is also contained in the Certificate Signing Request; and

(iii) that Organisation Certificate has neither expired nor been revoked.

Eligible Subscribers

L3.27 Where a Party has been an Eligible Subscriber in respect of any type of Organisation Certificate, but then ceases to be an Eligible Subscriber in respect of Organisation Certificates of that type, the DCC (acting in its capacity as Issuing OCA) shall as soon as reasonably practicable revoke every Organisation Certificate previously Issued to that Party for which it is no longer an Eligible Subscriber (subject to Section L16.1 (Supplier of Last Resort)).

Determinations by the Panel

L3.28 A Supplier Party (A) may apply to the Panel for the revocation of any Organisation Certificate Issued to another Supplier Party (B) which:

(a) has a keyUsage value of digitalSignature;

(b) includes one or more Market Participant Identifiers with which, in the opinion of Supplier Party A, Supplier Party B should not be associated; and

(c) at the time of the application has neither expired nor been revoked.

L3.29 Following an application made to the Panel by Supplier Party A under Section L3.28:

(a) Supplier Parties A and B shall provide the Panel with such information and assistance as it may reasonably request;

(b) the Panel shall, applying such criteria as it considers suitable for the purpose, determine whether it is appropriate for Supplier Party B to be associated with each Market Participant Identifier which is the subject of the application by Supplier Party A; and

(c) the Panel shall notify both Supplier Parties A and B of its determination.

L3.30 Where the Panel has determined that it is not appropriate for Supplier Party B to be associated with any Market Participant Identifier, it shall at the same time determine to require the revocation of each Organisation Certificate Issued to Supplier Party B which:

(a) has a keyUsage value of digitalSignature;

(b) includes that Market Participant Identifier; and

(c) at the time of the determination has not already expired or been revoked.

L3.31 The Panel shall notify the SMKI PMA of any determination made by it under Section L3.30.

L3.32 Where it is notified of any determination made by the Panel under Section L3.30, the SMKI PMA shall direct the DCC (acting in its capacity as Issuing OCA) to revoke each Organisation Certificate Issued to Supplier Party B which falls within the scope of that determination.

L3.33 Any determination made by the Panel in accordance with Section L3.29 or L3.30 maybe appealed to the Authority by either Supplier Party A or B, and the decision of the Authority shall be final and binding for the purposes of this Code.

Definitions

L3.34 For the purposes of this Section L3:

(a) “**keyUsage**” means the field referred to as such in the Organisation Certificate Policy;

(b) “**X520OrganizationalUnitName**” and “**subjectUniqueID**” mean those fields which are identified as such in the Organisation Certificate Profile at Annex B of the Organisation Certificate Policy; and

(c) “**accessControlBroker**” and “**wanProvider**”, when used in relation to the roles of the DCC, mean those roles which are identified as such, and have the meanings given to them, in the GB Companion Specification.

L4. THE SMKI SERVICE INTERFACE

DCC: Obligation to Maintain the SMKI Service Interface

L4.1 The DCC shall maintain the SMKI Service Interface in accordance with the SMKI Interface Design Specification and make it available, for sending and receiving communications in accordance with the SMKI Code of Connection, via DCC Gateway Connections, to:

(a) Authorised Subscribers; and

(b) (where applicable) Parties for the purpose of undertaking SMKI Entry Process Testing.

L4.2 The DCC shall ensure that the SMKI Service Interface is available at all times (subject to Planned Maintenance undertaken in accordance with Section H8.3):

(a) from the date on which the DCC is first obliged to provide the SMKI Services in accordance with Section L3 (The SMKI Services); and

(b) prior to that date, on such dates and to such extent as is necessary for the purpose of facilitating SMKI Entry Process Testing.

The SMKI Service Interface

L4.3 For the purposes of this Section L4, the "**SMKI Service Interface**" means a communications interface designed to allow communications to be sent between an Authorised Subscriber and the DCC for the purposes of the SMKI Services.

SMKI Interface Design Specification

L4.4 For the purposes of this Section L4, the "**SMKI Interface Design Specification**" shall be a SEC Subsidiary Document of that name which:

(a) shall specify the technical details of the SMKI Service Interface;

(b) shall include the protocols and technical standards that apply to the SMKI Service Interface;

(c) shall base those technical standards on PKIX/IETF/PKCS open standards, where:

(i) PKIX is the Public Key Infrastructure for X.509 Certificates, being an IETF set of standards for certificate and certificate revocation list profiles as specified in IETF RFC 5280;

(ii) the IETF is the Internet Engineering Task Force; and

(iii) PKCS is the Public Key Cryptography Standard;

(d) may set out the procedure by which an Authorised Subscriber and the DCC may communicate over the SMKI Service Interface, and may in particular specify any requirements on:

(i) an Authorised Subscriber which accesses, or is seeking to access, the SMKI Service Interface;

(ii) the DCC in relation to the provision of means of access to the SMKI Service Interface and/or any steps which must be taken by it in relation to communications made by an Authorised Subscriber and received by it over the SMKI Service Interface; and

(e) may specify limits on the use of the SMKI Service Interface, including in particular limits on the time or extent of its use, or conditions which must be satisfied for the purposes of its use at a specified time or to a specified extent.

SMKI Code of Connection

L4.5 For the purposes of this Section L4, the "**SMKI Code of Connection**" shall be a SEC Subsidiary Document of that name which:

(a) sets out the way in which an Authorised Subscriber may access the SMKI Service Interface;

(b) may specify limits on the use of the SMKI Service Interface, including in particular limits on the time or extent of its use, or conditions which must be satisfied for the purposes of its use at a specified time or to a specified extent;

(c) specifies the procedure by which an Authorised Subscriber and the DCC may communicate over the SMKI Service Interface; and

(d) includes a description of the way in which the mutual authentication and protection of communications taking place over the SMKI Service Interface will operate.

SMKI Interface Document Development

L4.6 The DCC shall develop drafts of the SMKI Interface Design Specification and SMKI Code of Connection:

(a) in accordance with the process set out at Section L4.7; and

(b) so that the drafts are available by no later than the date which falls six months prior to the commencement of Code Implementation SIT or such later date as may be specified by the Secretary of State.

L4.7 The process set out in this Section L4.7 for the development of drafts of the SMKI Interface Design Specification and SMKI Code of Connection is that:

(a) the DCC shall, in consultation with the Parties and such other persons as it considers appropriate, produce a draft of each document;

(b) where a disagreement arises with any person who is consulted with regard to any proposal as to the content of either document, the DCC shall endeavour to reach an agreed proposal with that person consistent with the purposes of the document;

(c) the DCC shall send a draft of each document to the Secretary of State as soon as is practicable after it is produced, and shall when doing so provide to the Secretary of State:

(i) a statement of the reasons why the DCC considers that draft document to be fit for purpose;

(ii) copies of the consultation responses received; and

(iii) a summary of any disagreements that arose during consultation and that have not been resolved by reaching an agreed proposal; and

(d) the DCC shall comply with any requirements in a direction given to it by the Secretary of State in relation to either draft document, including in particular:

(i) any requirement to produce and submit to the Secretary of State a further draft of either document; and

(ii) any requirement as to the process to be followed by the DCC (and the time within which that process shall be completed) prior to submitting a further such draft.

L5. THE SMKI REPOSITORY SERVICE

The SMKI Repository

L5.1 For the purposes of this Section L5, the "**SMKI Repository**" means a System for storing and (subject to the provisions of this Section) making available copies of the following:

(a) all Device Certificates;

(b) all DCA Certificates;

(c) all Organisation Certificates;

(d) all OCA Certificates;

(e) the IKI Certificates (to the extent required by the SMKI RAPP);

(f) any other IKI Certificates, and any ICA Certificates, which the DCC may from time to time consider appropriate;

(g) all versions of the Device Certificate Policy;

(h) all versions of the Organisation Certificate Policy;

(i) all versions of the IKI Certificate Policy;

(j) all versions of the SMKI RAPP;

(k) all versions of the SMKI Recovery Procedure;

(l) all versions of the SMKI Compliance Policy;

(m) the latest version of the Organisation CRL;

(n) the latest version of the Organisation ARL;

(o) such other documents or information (excluding any other public key infrastructure certificate) as may be specified by the SMKI PMA from time to time; and

(p) such other documents or information (excluding any other public key infrastructure certificate) as the DCC, in its capacity as the provider of the SMKI Services, may from time to time consider appropriate.

The SMKI Repository Service

L5.2 The DCC shall establish, operate, maintain and make available the SMKI Repository in accordance with the provisions of this Section L5 (the "**SMKI Repository Service**").

L5.3 The DCC shall ensure that the documents and information described in Section L5.1 may be lodged in the SMKI Repository:

(a) by itself, for the purpose of providing the SMKI Services or complying with any other requirements placed on it under the Code; and

(b) (except in the case of Certificates, the CRL and the ARL) by the SMKI PMA, or by the Code Administrator acting on its behalf, for the purpose of fulfilling its functions under the Code.

L5.4 The DCC shall ensure that no person may lodge documents or information in the SMKI Repository other than in accordance with Section L5.3.

L5.5 The DCC shall ensure that the SMKI Repository may be accessed for the purpose of viewing and/or obtaining a copy of any document or information stored on it by:

(a) any Party or RDP which reasonably requires such access in accordance, or for any purpose associated, with the Code;

(b) the Panel (or the Code Administrator acting on its behalf); and

(c) the SMKI PMA (or the Code Administrator acting on its behalf).

L5.6 The DCC shall ensure that no person may access documents or information in the SMKI Repository other than in accordance with Section L5.5 except where L5.6A applies.

L5.6A Any changes, alterations, modifications, deletions or replacement of any information or documentation contained in the SMKI Repository must be expressly approved by the SMKI PMA.

SMKI PMA: Role in relation to the SMKI Repository

L5.7 The SMKI PMA shall lodge each of the following documents in the SMKI Repository promptly upon the SMKI Repository Service first becoming available or (if later) the incorporation of that document into the Code:

(a) the Device Certificate Policy;

(b) the Organisation Certificate Policy;

(c) the IKI Certificate Policy; and

(d) the SMKI Compliance Policy.

L5.8 The SMKI PMA shall lodge in the SMKI Repository the modified version of each document referred to in Section L5.7 promptly upon any modification being made to that document in accordance with the Code.

L5.9 The SMKI PMA may require the DCC to lodge in the SMKI Repository such other documents or information as it may from time to time direct.

L5.10 Subject to Section L5.3, the SMKI PMA may lodge in the SMKI Repository such other documents or information as it may from time to time consider appropriate.

Parties: Duties in relation to the SMKI Repository

L5.11 Neither any Party nor RDP, or the SMKI PMA, may access the SMKI Repository for the purpose of viewing and/or obtaining a copy of any document or information stored on it except to the extent that it reasonably requires such access in accordance, or for any purpose associated, with the Code.

L6. THE SMKI REPOSITORY INTERFACE

DCC: Obligation to Maintain the SMKI Repository Interface

L6.1 The DCC shall maintain the SMKI Repository Interface in accordance with the SMKI Repository Interface Design Specification and make it available, via DCC Gateway Connections, to:

(a) the Parties and RDPs;

(b) the Panel (or the Code Administrator on its behalf); and

(c) the SMKI PMA (or the Code Administrator on its behalf),

to send and receive communications in accordance with the SMKI Repository Code of Connection and (where applicable) for the purpose of SMKI Entry Process Testing.

L6.2 The DCC shall ensure that the SMKI Repository Interface is available at all times (subject to Planned Maintenance undertaken in accordance with Section H8.3):

(a) from the date on which the DCC is first obliged to provide the SMKI Services in accordance with Section L3 (The SMKI Services); and

(b) prior to that date, on such dates and to such extent as is necessary for the purpose of facilitating SMKI Entry Process Testing.

The SMKI Repository Interface

L6.3 For the purposes of this Section L6, the "**SMKI Repository Interface**" means a communications interface designed to allow communications to be sent from and received by the SMKI Repository for the purposes of the SMKI Repository Service.

SMKI Repository Interface Design Specification

L6.4 For the purposes of this Section L6, the "**SMKI Repository Interface Design Specification**" shall be a SEC Subsidiary Document of that name which:

(a) specifies the technical details of the SMKI Repository Interface; and

(b) includes the protocols and technical standards that apply to the SMKI Repository Interface.

SMKI Repository Code of Connection

L6.5 For the purposes of this Section L6, the "**SMKI Repository Code of Connection**" shall be a SEC Subsidiary Document of that name which:

(a) sets out the way in which the Parties, the RDPs, the Panel and the SMKI PMA may access the SMKI Repository Interface;

(b) may specify limits on the use of the SMKI Repository Interface, including in particular limits on the time or extent of its use, or conditions which must be satisfied for the purposes of its use at a specified time or to a specified extent;

(c) specifies the procedure by which the Parties, the RDPs, the Panel and the SMKI PMA may communicate over the SMKI Repository Interface; and

(d) includes a description of the way in which the authentication and protection of communications taking place over the SMKI Repository Interface will operate.

SMKI Repository Interface Document Development

L6.6 The DCC shall develop drafts of the SMKI Repository Interface Design Specification and SMKI Repository Code of Connection:

(a) in accordance with the process set out at Section L6.7; and

(b) so that the drafts are available by no later than the date which falls six months prior to the commencement of Code Implementation SIT or such later date as may be specified by the Secretary of State.

L6.7 The process set out in this Section L6.7 for the development of drafts of the SMKI Repository Interface Design Specification and SMKI Repository Code of Connection is that:

(a) the DCC shall, in consultation with the Parties and such other persons as it considers appropriate, produce a draft of each document;

(b) where a disagreement arises with any person who is consulted with regard to any proposal as to the content of either document, the DCC shall endeavour to reach an agreed proposal with that person consistent with the purposes of the document;

(c) the DCC shall send a draft of each document to the Secretary of State as soon as is practicable after it is produced, and shall when doing so provide to the Secretary of State:

(i) a statement of the reasons why the DCC considers that draft document to be fit for purpose;

(ii) copies of the consultation responses received; and

(iii) a summary of any disagreements that arose during consultation and that have not been resolved by reaching an agreed proposal; and

(d) the DCC shall comply with any requirements in a direction given to it by the Secretary of State in relation to either document, including in particular:

(i) any requirement to produce and submit to the Secretary of State a further draft of either document; and

(ii) any requirement as to the process to be followed by the DCC (and the time within which that process shall be completed) prior to submitting a further such draft.

L7. SMKI AND REPOSITORY ENTRY PROCESS TESTS

Eligibility Generally

L7.1 A Party or RDP shall not be entitled to:

(a) apply to become an Authorised Subscriber for the purposes of any Certificate Policy; or

(b) access the SMKI Repository,

until that Party or RDP has successfully completed the SMKI and Repository Entry Process Tests for the purposes of paragraph (a) or (b) above (as applicable).

L7.2 Only persons that are Parties or RDPs are eligible to complete the SMKI and Repository Entry Process Tests.

SMKI and Repository Entry Guide

L7.3 The DCC shall establish and arrange for the publication on the Website of a guide to the SMKI and Repository Entry Process Tests, which shall identify any information that a Party or RDP is required to provide in support of its application to complete the SMKI and Repository Entry Process Tests (whether for the purposes of Section L7.1(a) or (b) or both).

SMKI and Repository Entry Process Tests

L7.4 A Party or RDP that wishes to complete the SMKI and Repository Entry Process Tests (whether for the purposes of Section L7.1(a) or (b) or both) must apply to the DCC in compliance with any requirements identified in the guide referred to in Section L7.3.

L7.5 On receipt of an application from a Party or RDP pursuant to Section L7.4, the DCC shall process that Party’s or RDP's application to complete the SMKI and Repository Entry Process Tests in accordance with this Section L7.

SMKI and Repository Entry Process Test Requirements

L7.6 A Party or RDP wishing to:

(a) become an Authorised Subscriber for the purposes of any Certificate Policy must have successfully completed the SMKI and Repository Entry Process Tests for that purpose; or

(b) access the SMKI Repository must have successfully completed the SMKI and Repository Entry Process Tests for that purpose.

L7.7 A Party or RDP will have successfully completed the SMKI and Repository Entry Process Tests for a particular purpose once that Party or RDP has received confirmation from the DCC that it has met the relevant requirements of Section L7.6.

L7.8 Once a Party or RDP has successfully completed the SMKI and Repository Entry Process Tests for a particular purpose, the DCC shall confirm the same to the Panel.

Network Parties and RDPs

L7.9 Each Network Party shall ensure that its Registration Data Provider (being the Network Party itself where that is deemed to be the case in accordance with the definition of Registration Data Provider) shall, when acting in its capacity as the Network Party's RDP to undertake the SMKI and Repository Entry Process Tests, comply with the obligations expressed to be placed on RDPs under Section H14 (Testing Services) and the SMKI and Repository Test Scenarios Document.

L7.10 Where more than one Network Party nominates the same Registration Data Provider, each of those Network Parties shall be jointly and severally liable for any failure by that RDP, when acting in its capacity as the Network Parties' RDP to undertake the SMKI and Repository Entry Process Tests, to comply with any of the obligations expressed to be placed on RDPs under Section H14 (Testing Services) and the SMKI and Repository Test Scenarios Document.

L8. SMKI PERFORMANCE STANDARDS AND DEMAND MANAGEMENT

SMKI Services: Target Response Times

L8.1 The DCC shall undertake the following activities within the following time periods (each such time period being, in respect of each such activity, the "**Target Response Time**" for that activity):

(a) in response to a single Certificate Signing Request, sending to an Eligible Subscriber either an Organisation Certificate or Device Certificate within 30 seconds of receipt of the Certificate Signing Request from that Eligible Subscriber over the SMKI Service Interface; and

(b) in response to a Batched Certificate Signing Request, sending to an Eligible Subscriber the number of Device Certificates that were requested:

(i) where the receipt of the Batched Certificate Signing Request from that Eligible Subscriber over the SMKI Service Interface occurred between the hours of 08:00 and 20:00 on any day, by no later than 08:00 on the following day; or

(ii) where the receipt of the Batched Certificate Signing Request from that Eligible Supplier over the SMKI Service Interface did not occur between the hours of 08:00 and 20:00, within 24 hours of the time of that receipt.

L8.2 For the purposes of Section L8.1, a "**Batched Certificate Signing Request**" is a single communication containing Certificate Signing Requests for the Issue of more than one but no more than 50,000 Device Certificates.

L8.3 For the purposes of Section L8.1, the concepts of 'sending' and 'receipt' are to be interpreted in accordance with the explanation of those concepts in the SMKI Interface Design Specification.

SMKI Repository Service: Target Response Time

L8.4 The DCC shall send to a Party, an RDP, the Panel or the SMKI PMA (as the case may be) a copy of any document or information stored on the SMKI Repository within 3 seconds of receipt of a request for that document from that person or body over the SMKI Repository Interface (and that time period shall be the “**Target Response Time**” for that activity).

L8.5 For the purposes of Section L8.4, the concepts of ‘sending’ and ‘receipt’ are to be interpreted in accordance with the explanation of those concepts in the SMKI Repository Interface Design Specification.

Code Performance Measures

L8.6 Each of the following performance measures constitute a Code Performance Measure (to which the following Target Service Level and Minimum Service Level will apply, measured over the following Performance Measurement Period):

No.	Code Performance Measure	Performance Measurement Period	Target Service Level	Minimum Service Level
7	Percentage of Certificates delivered within the applicable Target Response Time for the SMKI Services.	monthly	99%	96%
8	Percentage of documents stored on the SMKI Repository delivered within the applicable Target Response Time for the SMKI Repository Service.	monthly	99%	96%

SMKI Services: Managing Exceptional Demand

L8.7 An Authorised Subscriber will be considered to have exceptional demand if it is aware that the number of Certificate Signing Requests which it will send in a month will increase by 150% or more (50% above) compared to the average number of Certificate Signing Requests sent in each of the previous 3 months.

L8.8 Each Party which is an Authorised Subscriber in accordance with the Device Certificate Policy shall, if it becomes aware of exceptional demand, provide the DCC with a forecast of the number of Certificate Signing Requests which it will send in the relevant month.

L9. THE SMKI DOCUMENT SET

Obligations on the SMKI PMA

L9.1 The SMKI PMA shall exercise the functions that are allocated to it under and (in so far as they apply to it) comply with the requirements of the SMKI Document Set.

Obligations on SMKI Participants

L9.2 Each SMKI Participant shall (in so far as they apply to it) comply with the requirements of the SMKI SEC Documents.

The SMKI Document Set

L9.3 For the purposes of this Section L, the "**SMKI Document Set**" means:

(a) the SMKI SEC Documents;

(b) the Device CPS;

(c) the Organisation CPS; and

(d) the IKI CPS.

The SMKI SEC Documents

L9.4 For the purposes of this Section L, the "**SMKI SEC Documents**" means the provisions of the Code comprising:

(a) the following SEC Subsidiary Documents:

(i) the Device Certificate Policy;

(ii) the Organisation Certificate Policy;

(iii) the IKI Certificate Policy;

(iv) the SMKI Compliance Policy;

(v) the SMKI RAPP;

(vi) the SMKI Recovery Procedure;

(vii) the SMKI Interface Design Specification;

(viii) the SMKI Code of Connection;

(ix) the SMKI Repository Interface Design Specification;

(x) the SMKI Repository Code of Connection;

(xi) the SMKI and Repository Test Scenarios Document;

(b) the provisions of Sections L1 to L12; and

(c) every other provision of the Code which relates to the provision or the use of the SMKI Services or the SMKI Repository Service or to any matters directly arising from or affecting the provision or the use of those Services.

The Registration Authority Policies and Procedures: Document Development

L9.5 The DCC shall develop a draft of the SMKI RAPP:

(a) to make provision for such matters as are specified in the Certificate Policies as being matters provided for in the SMKI RAPP;

(b) to make provision for such other matters as are necessary or appropriate in relation to the exercise of its functions as the Registration Authority;

(c) to make provision for such matters as are necessary or appropriate in relation to Test Certificates that are being made available to Testing Participants;

(d) to make such provision as the DCC may consider appropriate in relation to the means by which the identity and authorisation of individuals and Parties may be verified for the purposes of the DCCKI Services (in addition to any such provision made in respect of the SMKI Services);

(e) in accordance with the process set out at Section L9.6; and

(f) so that the draft is available by no later than the date which falls six months prior to the commencement of Code Implementation SIT or such later date as may be specified by the Secretary of State.

L9.6 The process set out in this Section L9.6 for the development of a draft of the SMKI RAPP is that:

(a) the DCC shall, in consultation with the Parties and such other persons as it considers appropriate, produce a draft of the SMKI RAPP;

(b) where a disagreement arises with any person who is consulted with regard to any proposal as to the content of the SMKI RAPP, the DCC shall endeavour to reach an agreed proposal with that person consistent with the purposes of the SMKI RAPP specified in Section L9.5;

(c) the DCC shall send a draft of the SMKI RAPP to the Secretary of State as soon as is practicable after it is produced, and shall when doing so provide to the Secretary of State:

(i) a statement of the reasons why the DCC considers that draft to be fit for purpose; and

(ii) a summary of any disagreements that arose during consultation and that have not been resolved by reaching an agreed proposal; and

(d) the DCC shall comply with any requirements in a direction given to it by the Secretary of State in relation to the draft of the SMKI RAPP, including in particular:

(i) any requirement to produce and submit to the Secretary of State a further draft of the document; and

(ii) any requirement as to the process to be followed by the DCC (and the time within which that process shall be completed) prior to submitting a further such draft.

The Device Certification Practice Statement

L9.7 The DCC shall establish, give effect to, maintain and comply with a document which shall be known as the "**Device CPS**".

L9.8 The Device CPS shall be a document which:

(a) sets out the policies and procedures of the DCC designed to ensure that it will comply with the requirements of the Device Certificate Policy;

(b) incorporates the detailed operating procedures to be used by the DCC for the purposes of its compliance with the requirements of that Policy;

(c) incorporates such other provisions as may be required by or in accordance with that Policy or any other part of the Code; and

(d) is approved by the SMKI PMA as appropriate for these purposes.

L9.9 For the purposes of the approval of the Device CPS by the SMKI PMA in accordance with Section L9.8(d):

(a) the DCC shall submit an initial draft of the Device CPS to the SMKI PMA by no later than the date which falls three months prior to the commencement of Code Implementation SIT or such later date as may be agreed by the SMKI PMA;

(b) the SMKI PMA shall review the initial draft of the Device CPS and shall:

(i) approve the draft, which shall become the Device CPS; or

(ii) state that it will approve the draft subject to the DCC first making such amendments to the document as it may direct; and

(c) the DCC shall make any amendments to the draft Device CPS that may be directed by the SMKI PMA, and the amended draft shall become the Device CPS.

L9.10 The DCC shall keep the Device CPS under review, and shall in particular carry out a review of the Device CPS whenever (and to the extent to which) it may be required to so by the SMKI PMA.

L9.11 Following any review of the Device CPS:

(a) the DCC may propose amendments to it, which it shall submit to the SMKI PMA for its approval; and

(b) those amendments may be made only to the extent to which the SMKI PMA has approved them.

L9.12 Both the DCC and the SMKI PMA shall treat the Device CPS as confidential.

The Organisation Certification Practice Statement

L9.13 The DCC shall establish, give effect to, maintain and comply with a document which shall be known as the "**Organisation CPS**".

L9.14 The Organisation CPS shall be a document which:

(a) sets out the policies and procedures of the DCC designed to ensure that it will comply with the requirements of the Organisation Certificate Policy;

(b) incorporates the detailed operating procedures to be used by the DCC for the purposes of its compliance with the requirements of that Policy;

(c) incorporates such other provisions as may be required by or in accordance with that Policy or any other part of the Code; and

(d) is approved by the SMKI PMA as appropriate for these purposes.

L9.15 For the purposes of the approval of the Organisation CPS by the SMKI PMA in accordance with Section L9.14(d):

(a) the DCC shall submit an initial draft of the Organisation CPS to the SMKI PMA by no later than the date which falls three months prior to the commencement of Code Implementation SIT or such later date as may be agreed by the SMKI PMA;

(b) the SMKI PMA shall review the initial draft of the Organisation CPS and shall:

(i) approve the draft, which shall become the Organisation CPS; or

(ii) state that it will approve the draft subject to the DCC first making such amendments to the document as it may direct; and

(c) the DCC shall make any amendments to the draft Organisation CPS that may be directed by the SMKI PMA, and the amended draft shall become the Organisation CPS.

L9.16 The DCC shall keep the Organisation CPS under review, and shall in particular carry out a review of the Organisation CPS whenever (and to the extent to which) it may be required to so by the SMKI PMA.

L9.17 Following any review of the Organisation CPS:

(a) the DCC may propose amendments to it, which it shall submit to the SMKI PMA for its approval; and

(b) those amendments may be made only to the extent to which the SMKI PMA has approved them.

L9.18 Both the DCC and the SMKI PMA shall treat the Organisation CPS as confidential.

The IKI Certification Practice Statement

L9.19 The DCC shall establish, give effect to, maintain and comply with a document which shall be known as the "**IKI CPS**".

L9.20 The IKI CPS shall be a document which:

(a) sets out the policies and procedures of the DCC designed to ensure that it will comply with the requirements of the IKI Certificate Policy;

(b) incorporates the detailed operating procedures to be used by the DCC for the purposes of its compliance with the requirements of that Policy;

(c) incorporates such other provisions as may be required by or in accordance with that Policy or any other part of the Code; and

(d) is approved by the SMKI PMA as appropriate for these purposes.

L9.21 For the purposes of the approval of the IKI CPS by the SMKI PMA in accordance with Section L9.20(d):

(a) the DCC shall submit an initial draft of the IKI CPS to the SMKI PMA by no later than the date which falls one month prior to the commencement of Code Implementation SIT or such later date as may be agreed by the SMKI PMA;

(b) the SMKI PMA shall review the initial draft of the IKI CPS and shall:

(i) approve the draft, which shall become the IKI CPS; or

(ii) state that it will approve the draft subject to the DCC first making such amendments to the document as it may direct; and

(c) the DCC shall make any amendments to the draft IKI CPS that may be directed by the SMKI PMA, and the amended draft shall become the IKI CPS.

L9.22 The DCC shall keep the IKI CPS under review, and shall in particular carry out a review of the IKI CPS whenever (and to the extent to which) it may be required to so by the SMKI PMA.

L9.23 Following any review of the IKI CPS:

(a) the DCC may propose amendments to it, which it shall submit to the SMKI PMA for its approval; and

(b) those amendments may be made only to the extent to which the SMKI PMA has approved them.

L9.24 Both the DCC and the SMKI PMA shall treat the IKI CPS as confidential.

Enquiries in relation to the SMKI Document Set

L9.25 The DCC shall respond within a reasonable time to any reasonable request for information made by a Party or RDP in relation to the SMKI Services, the SMKI Repository Services or the SMKI Document Set, but excluding any request for a copy of any document or information which can be accessed through the SMKI Repository.

L10. THE SMKI RECOVERY PROCEDURE

The SMKI Recovery Procedure

L10.1 For the purposes of this Section L10, the "**SMKI Recovery Procedure**" shall be a SEC Subsidiary Document of that name which sets out, in relation to any incident in which a Relevant Private Key is (or is suspected of being) Compromised:

(a) the mechanism by which Parties and RDPs may notify the DCC and the DCC may notify Parties, RDPs and the SMKI PMA that the Relevant Private Key has been (or is suspected of having been) Compromised;

(b) procedures relating to the use of the Recovery Private Key and Contingency Private Key (and the use of the Contingency Symmetric Key) where such use has been required in accordance with a decision of the SMKI PMA;

(c) procedures relating to:

(i) the distribution of new Root OCA Certificates and Organisation Certificates to Devices; and

(ii) the coordination of the submission of Certificate Signing Requests by Eligible Subscribers following the replacement of any OCA Certificate;

(d) steps to be taken by the DCC, the Parties (or any of them, whether individually or by Party Category), RDPs, the SMKI PMA (or any SMKI PMA Members) and the Panel (or any Panel Members), including in particular in respect of:

(i) notification of the Compromise (or suspected Compromise); and

(ii) the process for taking steps to avoid or mitigate the adverse effects of, or to recover from, the (actual or suspected) Compromise, which steps may differ depending on the Relevant Private Key that has been (or is suspected of having been) Compromised and the nature and extent of the (actual or suspected) Compromise and the adverse effects arising from it; and

(e) arrangements to be made preparatory to and for the purpose of ensuring the effective operation of the matters described in paragraphs (a) to (d), and the associated technical solutions employed by the DCC, including for their periodic testing.

L10.2 The SMKI Recovery Procedure:

(a) shall make provision for the use of the Recovery Private Key and Contingency Private Key (and the use of the Contingency Symmetric Key) only where such use has been required in accordance with a decision of the SMKI PMA;

(b) shall make provision for the DCC, if it has reason to believe that the use of the Recovery Private Key or Contingency Private Key (including in the latter case the use of the Contingency Symmetric Key) is likely to be required by the SMKI PMA, to take or instruct any Party, any SMKI PMA Member or any Panel Member to take such preparatory steps in respect of that use as it considers appropriate; and

(c) may make provision:

(i) that, in specified circumstances, certain requirements of the SMKI Recovery Procedure, or of decisions made under and in accordance with the provisions of the SMKI Recovery Procedure, may take precedence over the other provisions of the Code;

(ii) for the operation of procedures which, in specified circumstances, require that decisions over whether or not to take certain steps are referred to the SMKI PMA for its determination;

(iii) for the SMKI PMA to require any Party to nominate individuals for the purpose of performing specified tasks.

L10.3 Where the DCC follows any of the procedures specified in the SMKI Recovery Procedure, it shall, as soon as is reasonably practicable, notify the SMKI PMA of the steps that it has taken and provide such additional supporting information as the SMKI PMA reasonably requests.

SMKI Recovery Procedure: Obligations

L10.4 The DCC, each Party, the SMKI PMA (and SMKI PMA Members) and the Panel (and Panel Members) shall comply, in so far as applicable to it (or them), with any requirements set out in the SMKI Recovery Procedure.

L10.5 Any SMKI PMA Member or Panel Member who is appointed by (respectively) the SMKI PMA or Panel to carry out a specific role in respect of the SMKI Recovery Procedure must take reasonable steps to act in accordance with any instructions given to him by the SMKI PMA or Panel (as the case may be) in relation to the way in which that role is to be carried out.

L10.6 The DCC shall reimburse the reasonable costs of any Party which that Party can demonstrate were incurred by it solely and directly in consequence of actions taken by it to support the maintenance of the procedures and arrangements set out in the SMKI Recovery Procedure, and which it would not otherwise have incurred.

SMKI Recovery Procedure: Document Development

L10.7 The DCC shall develop a draft of the SMKI Recovery Procedure:

(a) in accordance with the process set out at Section L10.8; and

(b) so that the draft is available by no later than the date which falls six months prior to the commencement of Code Implementation SIT or such later date as may be specified by the Secretary of State.

L10.8 The process set out in this Section L10.8 for the development of a draft of the SMKI Recovery Procedure is that:

(a) the DCC shall, in consultation with the Parties, the SMKI PMA and such other persons as it considers appropriate, produce a draft of the SMKI Recovery Procedure;

(b) where a disagreement arises with any person who is consulted with regard to any proposal as to the content of the SMKI Recovery Procedure, the DCC shall endeavour to reach an agreed proposal with that person consistent with the purposes of the SMKI Recovery Procedure specified in Section L10.1;

(c) the DCC shall send a draft of the SMKI Recovery Procedure to the Secretary of State as soon as is practicable after it is produced, and shall when doing so provide to the Secretary of State:

(i) a statement of the reasons why the DCC considers that draft to be fit for purpose; and

(ii) a summary of any disagreements that arose during consultation and that have not been resolved by reaching an agreed proposal; and

(d) the DCC shall comply with any requirements in a direction given to it by the Secretary of State in relation to the draft of the SMKI Recovery Procedure, including in particular:

(i) any requirement to produce and submit to the Secretary of State a further draft of the document; and

(ii) any requirement as to the process to be followed by the DCC (and the time within which that process shall be completed) prior to submitting a further such draft.

The SMKI Recovery Key Guidance

L10.9 For the purposes of this Section L10, the "**SMKI Recovery Key Guidance**" shall be a document of that name which makes such provision as is appropriate, in relation to any incident in which a Relevant Private Key is (or is suspected of being) Compromised, for any one or more of the following:

(a) any factors which shall be taken into account by the SMKI PMA in deciding whether or not to require the use of the Recovery Private Key or Contingency Private Key (including in the latter case the use of the Contingency Symmetric Key);

(b) any other factors which may in particular be taken into account by the SMKI PMA for the purposes of that decision;

(c) any weighting or order of priority which shall, or may, be given by the SMKI PMA to any of the factors referred to in paragraphs (a) and (b); and

(d) any criteria that are to be applied by the SMKI PMA, any approach that is to be followed by it, or any steps that are to be taken by it, prior to making a decision whether or not to require the use of the Recovery Private Key or Contingency Private Key (including in the latter case the use of the Contingency Symmetric Key).

Recovery Key Guidance: Obligations

L10.10 The SMKI PMA:

(a) shall act in accordance with the SMKI Recovery Key Guidance in making any decision whether or not to require the use of the Recovery Private Key or Contingency Private Key (including in the latter case the use of the Contingency Symmetric Key); and

(b) may request such information and assistance from the DCC, the Security Sub- Committee or any Party as it reasonably considers appropriate for the purposes of making any such decision or ensuring that it will be prepared to make any such decision that may fall to be made by it at a future date.

L10.11 The DCC, each other Party, and the Security Sub-Committee shall promptly provide the SMKI PMA with such information and assistance as may be requested in accordance with Section L10.10.

L10.12 The DCC shall, where requested to do so, reimburse the reasonable costs of any Party associated with the provision of assistance in accordance with Section L10.11.

Recovery Key Guidance: Document Development

L10.13 The SMKI PMA shall:

(a) develop the SMKI Recovery Key Guidance, and for that purpose:

(i) consult with the DCC, the Security Sub-Committee, the Parties, the Secretary of State and the Authority; and

(ii) have regard to the views of each person consulted by it prior to determining the content of the document;

(b) periodically review the SMKI Recovery Key Guidance, and in particular carry out a review whenever (and to the extent to which) it may be required to do so by the Panel or the Authority;

(c) where, following any review, it proposes to amend the SMKI Recovery Key Guidance:

(i) consult the DCC, the Security Sub-Committee, the Parties and the Authority in relation to the proposed amendments; and

(ii) have regard to the views of each person consulted by it prior to making any amendments to the document; and

(d) publish the SMKI Recovery Key Guidance, as initially determined by it and on each amendment made to that document from time to time.

Recovery Events and Recovery Costs

Recovery Events

L10.14 For the purposes of this Section L10, a "**Recovery Event**" is an event that shall be taken to have occurred when the circumstances described in either Section L10.15 or L10.16 exist.

L10.15 The circumstances described in this Section L10.15 are that:

(a) the DCC has notified the SMKI PMA that a Relevant Private Key has been (or is suspected of having been) Compromised; and

(b) in consequence of that (actual or suspected) Compromise, the SMKI PMA has decided to require the use of the Recovery Private Key or Contingency Private Key (including in the latter case the use of the Contingency Symmetric Key) in accordance with the SMKI Recovery Procedure.

L10.16 The circumstances described in this Section L10.16 are that:

(a) the DCC has notified the SMKI PMA that a Relevant Private Key has been (or is suspected of having been) Compromised;

(b) the SMKI PMA has been provided with (or otherwise obtained) evidence that:

(i) attempts have been made, by means of sending appropriate Commands, to replace the Data comprising part of the Device Security Credentials of Relevant Devices which derive from any Organisation Certificate or OCA Certificate which is (or is suspected of being) Compromised; or

(ii) it was not feasible or appropriate for any such attempt to be made; and

(c) the SMKI PMA has decided not to require the use of the Recovery Private Key or Contingency Private Key (including in the latter case the use of the Contingency Symmetric Key).

Recovery Costs

L10.17 For the purposes of this Section L10, the "**Recovery Costs**" shall be such costs as are reasonably incurred in consequence of a Recovery Event (and which would not otherwise have incurred) by any Party:

(a) in respect of the use of the Recovery Private Key or Contingency Private Key (including in the latter case the use of the Contingency Symmetric Key) in accordance with the requirement of the SMKI PMA; and

(b) in taking such action as is necessary, where the Recovery Private Key or Contingency Private Key (including in the latter case the Contingency Symmetric Key) has not been used or has been used unsuccessfully, to replace:

(i) Relevant Devices for which that Party is the Responsible Supplier; or

(ii) the Data comprising part of the Device Security Credentials of such Relevant Devices which derive from any Organisation Certificate or OCA Certificate which is (or is suspected of being) Compromised.

Payment of Recovery Costs by the DCC

L10.18 Where any Party incurs Recovery Costs, it may submit to the DCC a request to be recompensed in respect of those costs.

L10.19 Where any Party wishes to submit a request in accordance with Section L10.18, it shall:

(a) within three months of the Recovery Event, notify the DCC of its intention to do so;

(b) unless, at the same time as notifying the DCC of that intention it also notifies the DCC of the total amount of the costs in respect of which it requests to be recompensed:

(i) provide to the DCC at that time its best estimate of the likely amount of those costs; and

(ii) at least once in every subsequent period of three months, until such time as it notifies the DCC of the total amount of the costs in respect of which it requests to be recompensed, provide to the DCC an updated best estimate of the likely amount of those costs; and

(c) as soon as possible, and in any event within three months of the date on which it ceases to incur Recovery Costs, notify the DCC of the total amount of the costs in respect of which it requests to be recompensed.

L10.20 A Party giving notice to the DCC in accordance with Section L10.19 shall:

(a) subject to paragraph (b), provide to the DCC such evidence in respect of the amount of the Recovery Costs incurred by that Party:

(i) as the DCC may reasonably require;

(ii) by such dates as the DCC may reasonably specify; or

(b) where the Panel considers the matter either of its own motion or on a referral by the Party or the DCC, provide to the DCC such evidence relating to the amount of the costs incurred by that Party:

(i) as the Panel may determine is reasonably required;

(ii) by such dates as the Panel may reasonably specify.

L10.21 The evidence referred to in Section L10.20 may include in particular, if the DCC or the Panel (as the case may be) determines that it is reasonably required, the report of an independent auditor verifying that the amount requested by a Party represents a fair and accurate statement of the Recovery Costs incurred by that Party.

L10.22 On receipt by it of a request from a Party to be recompensed in respect of Recovery Costs, the DCC shall, where it is satisfied that the amount of the costs requested by that Party is adequately supported by the evidence provided to it in accordance with Section L10.20, pay to the Party that amount.

L10.23 Where the DCC has any question whether the evidence provided to it by a Party is adequate to support the amount of the costs requested:

(a) it shall refer that question to the Panel for its determination; and

(b) the Panel shall determine that question by directing that the DCC shall pay to the Party the full amount requested or only part of that amount (in a sum that is specified by the Panel), or shall make no payment to that Party.

L10.24 Where the amount of the Recovery Costs requested by any Party is (whether alone or taken together with amounts requested by any other Parties in relation to the same Recovery Event) for a sum exceeding that which is determined from time to time by the Panel, following consultation with the Parties and the Authority, for the purposes of this Section L10.24:

(a) the DCC may refer to the Panel, for its determination, the question of the dates on which the payments of the amounts requested shall be made;

(b) the Panel shall determine the dates on which those payments shall be made, and may in particular determine that:

(i) different Parties shall be paid at different times; and

(ii) any amount which is to be paid to a Party shall be paid in instalments at different times; and

(c) the Panel shall consider whether to submit any Draft Proposal in relation to the Charging Methodology (taking into account whether it is proposed by the Authority to make any adjustment to the allowable revenues of the DCC, or by the DCC to amend the Charging Statement).

Breach of the Code by the Relevant Subscriber

L10.25 Where a Recovery Event occurs, and where the Relevant Subscriber is the DCC, the DCC shall be deemed to be in breach of:

(a) where the (actual or suspected) Compromise is to an Organisation Certificate, Section L11.9 (Organisation and IKI Certificates: Protection of Private Keys); or

(b) where the (actual or suspected) Compromise is to an OCA Certificate, Part 6.2.1 of the Organisation Certificate Policy (Cryptographic Module Standards and Controls).

L10.26 Where a Recovery Event occurs, and where the Relevant Subscriber is any Party other than the DCC, that Party shall be deemed to be in breach of Section L11.9 (Organisation and IKI Certificates: Protection of Private Keys), unless the (actual or suspected) Compromise to the Relevant Private Key which gave rise to the Recovery Event was due to the (actual or suspected) Compromise of an OCA Certificate.

L10.27 Where a Relevant Subscriber is, by virtue of Section L10.25 or L10.26, deemed to be in breach of a provision of this Code, it shall cease to be so deemed (and no such breach shall be treated as having occurred) where:

(a) within three months of the date of the Recovery Event it refers the matter to the Panel;

(b) following that referral it demonstrates to the reasonable satisfaction of the Panel, that the (actual or suspected) Compromise to the Relevant Private Key which gave rise to the Recovery Event was not due to its breach of Section L11.9 or of Part 6.2.1 of the Organisation Certificate Policy (as the case may be); and

(c) the Panel determines accordingly that no such breach occurred.

L10.28 In all circumstances other than those described in Section L10.27, and subject to the provisions of Section L10.29, where a breach is deemed to have occurred in accordance with Section L10.25 or L10.26, that shall be treated as a final and binding determination of its occurrence for the purposes of this Code.

Appeal to the Authority

L10.29 Any decision made by the Panel in accordance with Section L10.20, L10.23, L10.24 or L10.27 may be appealed to the Authority, whose decision shall be final and binding for the purposes of this Code.

Further Use of the Recovery Private Key

L10.29A Subject to Section L10.29B where, to the extent, and (where relevant) in the manner directed to do so by the SMKI PMA, the DCC shall use the Recovery Private Key to replace (in whole or in part) the data comprising the Device Security Credentials held on or in relation to one or more specified Devices that form part of one or more Enrolled Smart Metering Systems with data from one or more specified Organisation Certificates.

L10.29B A Recovery Key Direction may only be given by the SMKI PMA to the DCC in the following circumstances:

(a) the SMKI PMA believes that the data comprising the Device Security Credentials of one or more Devices that form part of one or more Enrolled Smart Metering Systems is incorrectly populated, and that this could be rectified through the use of the Recovery Private Key; and

(b) the SMKI PMA reasonably believes that it is not possible to rectify the incorrectly populated data using the Private Key(s) associated with the Public Key(s) contained in the Organisation Certificate(s) from which the incorrectly populated data originated because those Private Key(s) is/are Unavailable Private Keys; and

(c) the SMKI PMA has decided to direct the DCC to use the Recovery Private Key after taking into account the costs and benefits of doing so.

L10.29C As soon as reasonably practicable after the Recovery Private Key has been used pursuant to a Recovery Key Direction:

(a) the DCC shall provide a report to the SMKI PMA setting out the results of the actions that it has taken; and

(b) the SMKI PMA shall provide a report to the Panel explaining the circumstances which led it to decide to make a Recovery Key Direction and inform the Panel of the results of the DCC's actions.

Definitions

L10.30 For the purposes of this Section L10:

(a) a "**Relevant Device**" means a Device:

(i) which has, or had immediately prior to a Recovery Event, an SMI Status of 'commissioned'; and

(ii) the Device Security Credentials of which are populated with, or are reasonably believed immediately prior to a Recovery Event to have been populated with, Data from an Organisation Certificate or OCA Certificate which has been (or is suspected of having been) Compromised as a result of an (actual or suspected) Compromise to the Relevant Private Key which gave rise to the Recovery Event;

(b) the "**Relevant Subscriber**" means, where a Recovery Event has occurred, the Subscriber for an Organisation Certificate or OCA Certificate which has been (or is suspected of having been) Compromised as the result of an (actual or suspected) Compromise to the Relevant Private Key which gave rise to the Recovery Event;

(c) a "**Relevant Private Key**" means:

(i) the Contingency Symmetric Key;

(ii) a Private Key which is associated with a Public Key contained in any Organisation Certificate or OCA Certificate, Data from which is used to populate the Device Security Credentials of a Device comprising part of an Enrolled Smart Metering System;

(iii) a Private Key which is associated with a Public Key contained in any Organisation Certificate, Data from which is used to populate part of any Device Security Credentials held by an S1SP;

(iv) a Private Key which was used as part of the process of Issuing any OCA Certificate or Organisation Certificate referred to in paragraph (ii) or (iii) above;

(v) a Private Key which is used to Digitally Sign any XML Document, and which is associated with a Public Key that is contained within any Organisation Certificate; or

(vi) a Private Key which is associated with a Public Key contained in any certificate issued in accordance with an S1SPKI Certificate Policy, and which is determined by the SMKI PMA as being a Private Key for the purposes of this paragraph;

(d) a "**Recovery Key Pair**" means a Key Pair established by the DCC for the purposes of the replacement of Organisation Certificates on Devices after a Relevant Private Key has been Compromised, and:

(i) a "**Recovery Private Key**" means the Private Key which is part of that Key Pair; and

(ii) a "**Recovery Certificate**" means an Organisation Certificate Issued by the OCA and containing the Public Key which is part of that Key Pair;

(e) a "**Recovery Key Direction**" means a direction issued by the SMKI PMA to the DCC pursuant to Section L10.29A; and

(f) an "**Unavailable Private Key**" means a Private Key that has been destroyed or is unavailable for use because the Subscriber for the Organisation Certificate which contains the associated Public Key has never been, or has ceased to be a DCC User.

L11. THE SUBSCRIBER OBLIGATIONS

Certificate Signing Requests

L11.1 Each Eligible Subscriber shall ensure that all of the information contained in each Certificate Signing Request made by it is true and accurate.

L11.2 No Eligible Subscriber may make a Certificate Signing Request which contains:

(a) any information that constitutes a trade mark, unless it is the holder of the Intellectual Property Rights in relation to that trade mark; or

(b) any confidential information which would be contained in a Certificate Issued in response to that Certificate Signing Request.

L11.3 Each Eligible Subscriber shall ensure that either:

(a) where appropriate, in the case of a Certificate Signing Request for the Issue of an IKI Certificate, that Certificate Signing Request has been generated using a Cryptographic Credential Token that was provided by the DCC to the Eligible Subscriber in accordance with the SMKI RAPP; or

(b) in every other case, the Public Key that is included within a Certificate Signing Request is part of a Key Pair that has been generated using random numbers which are such as to make it computationally infeasible to regenerate that Key Pair even with knowledge of when and by means of what equipment it was generated.

L11.4 No Eligible Subscriber may make a Certificate Signing Request for the Issue of:

(a) a Device Certificate or DCA Certificate which contains the same Public Key as a Public Key which that Eligible Subscriber knows to be contained in any other Device Certificate or DCA Certificate;

(b) subject to Section 11.4A, an Organisation Certificate or OCA Certificate which contains the same Public Key as a Public Key which that Eligible Subscriber knows to be contained in any other Organisation Certificate or OCA Certificate (except in the case of the Root OCA Certificate to the extent to which it is expressly permitted in accordance with the Organisation Certificate Policy); or

(c) an IKI Certificate or ICA Certificate which contains the same Public Key as a Public Key which that Eligible Subscriber knows to be contained in any other IKI Certificate or ICA Certificate.

L11.4A Subject to 11.4B, the DCC may submit a Certificate Signing Request for, and may Issue, an Organisation Certificate that has the same Public Key as an existing Organisation Certificate.

L11.4B The circumstances in which 11.4A applies are:

(a) that the SMKI PMA (having taken into account the views of the Security Sub-Committee) has given approval for a Certificate to be Issued that contains the same Public Key as an existing Organisation Certificate; and

(b) the Remote Party Role Code for that Certificate is either: "recovery", "transitionalCoS", "wanProvider", or "accessControlBroker".

Subscribing for or Rejecting Organisation Certificates

L11.5 Where any Organisation Certificate is Issued to an Eligible Subscriber in response to a Certificate Signing Request, that Eligible Subscriber shall:

(a) establish whether the information contained in that Certificate is consistent with information that was contained in the Certificate Signing Request;

(b) if it identifies that the Certificate contains any information which is untrue or inaccurate:

(i) reject that Certificate; and

(ii) immediately inform the DCC that it rejects the Certificate and give to the DCC its reasons for doing so; and

(c) where it does not reject the Certificate, become a Subscriber for that Certificate.

Subscribing for or Rejecting Device Certificates

L11.6 Where any Device Certificate is Issued to an Eligible Subscriber in response to a Certificate Signing Request, that Eligible Subscriber shall:

(a) take reasonable steps to establish whether the information contained in that Certificate is consistent with information that was contained in the Certificate Signing Request;

(b) if it identifies that the Certificate contains any information which is untrue or inaccurate:

(i) reject that Certificate; and

(ii) immediately inform the DCC that it rejects the Certificate and give to the DCC its reasons for doing so; and

(c) where it does not reject the Certificate, become a Subscriber for that Certificate.

Subscribing for or Rejecting IKI Certificates

L11.7 Where any IKI Certificate is Issued to an Eligible Subscriber in response to a Certificate Signing Request, that Eligible Subscriber shall:

(a) establish whether the information contained in that Certificate is consistent with information that was contained in the Certificate Signing Request;

(b) if it identifies that the Certificate contains any information which is untrue or inaccurate:

(i) reject that Certificate;

(ii) immediately inform the DCC that it rejects the Certificate and give to the DCC its reasons for doing so; and

(c) where it does not reject the Certificate, become a Subscriber for that Certificate.

Use of Certificates and Key Pairs

L11.8 Each Subscriber shall ensure that it does not use any Certificate, Public Key contained within a Certificate, or Private Key associated with a Public Key contained in a Certificate, that is held by it other than for the purposes of creating, sending, receiving and processing communications sent to and from Devices and the DCC pursuant to the Code.

Organisation and IKI Certificates: Protection of Private Keys

L11.9 Each Subscriber shall (in addition, if it is the DCC, a User or an RDP, to its obligations under Section G (Security)) take reasonable steps to ensure that no Compromise occurs to any:

(a) Private Key which is associated with a Public Key contained in an Organisation Certificate or IKI Certificate for which it is the Subscriber; or

(b) Secret Key Material associated with that Private Key.

Organisation Certificates: Expiry of Validity Period

L11.10 Each Subscriber shall, prior to the expiry of the Validity Period of an Organisation Certificate or OCA Certificate for which it is the Subscriber:

(a) request a replacement for that Certificate by applying for the Issue of a new Organisation Certificate or OCA Certificate in accordance with the provisions of the Organisation Certificate Policy; and

(b) ensure that any Data from that Certificate which are used to populate the Device Security Credentials of any Device are replaced by Data from the new Certificate Issued to it by the OCA.

Organisation Certificates: Gas Network Parties

L11.11 Where a Subscriber is a Gas Network Party and intends to cease to be a DCC User, it must:

(a) ensure that the Gas Network Operator (GNO) Certificates in each of its SMETS2+ Gas Proxy Function (GPF) Trust Anchor Cells are replaced with Access Control Broker (ACB) Certificates.

(b) not make any further Certificate Signing Requests until such time as it returns to being a DCC User.

L12. RELYING PARTY OBLIGATIONS

Relying Parties

L12.1 For the purposes of this Section L12, a 'Relying Party' in relation to an Organisation Certificate, OCA Certificate, IKI Certificate or ICA Certificate means any Party or RDP which relies on the Certificate for the purposes of creating, sending, receiving or processing communications sent to and from a Device or another Party or RDP pursuant to this Code.

L12.2 For the purposes of Section L12.1, a Relying Party shall be deemed to include:

(a) in the case of a Device which relies on a Certificate, the Responsible Supplier for that Device; and

(b) in the case of a Communications Hub Function or Gas Proxy Function which relies on a Certificate, the DCC.

Duties in relation to Organisation Certificates, OCA Certificates, IKI Certificates and ICA Certificates

L12.3 Each Relying Party shall:

(a) before relying on any Organisation Certificate:

(i) Check Cryptographic Protection in respect of the Organisation CRL on the SMKI Repository; and

(ii) where that Certificate is shown on the Organisation CRL as having been revoked, not rely on the Certificate;

(b) before relying on any OCA Certificate:

(i) Check Cryptographic Protection in respect of the Organisation ARL on the SMKI Repository; and

(ii) where that Certificate is shown on the Organisation ARL as having been revoked, not rely on the Certificate;

(c) before relying on any IKI Certificate:

(i) Check Cryptographic Protection in respect of the IKI CRL; and

(ii) where that Certificate is shown on the IKI CRL as having been revoked, not rely on the Certificate; and

(d) before relying on any ICA Certificate:

(i) Check Cryptographic Protection in respect of the IKI ARL; and

(ii) where that Certificate is shown on the IKI ARL as having been revoked, not rely on the Certificate.

L12.4 No Relying Party may rely on an Organisation Certificate or IKI Certificate where the Validity Period of that Certificate has expired.

L12.5 No Relying Party may rely on an Organisation Certificate, OCA Certificate, IKI Certificate or ICA Certificate where it suspects that the Certificate has been Compromised.

L12.6 Each Relying Party shall take reasonable steps, by means of appropriate Systems, to verify Digital Signatures, Check Cryptographic Protection, Confirm Validity and perform other appropriate cryptographic operations before relying on any Organisation Certificate, OCA Certificate, IKI Certificate or ICA Certificate.

L13. DCC KEY INFRASTRUCTURE

The DCCKI Services

The DCCKI Services

L13.1 For the purposes of this Section L13, the "**DCCKI Services**" means all of the activities undertaken by the DCC in its capacity as the DCCKI Certification Authority in accordance with the applicable requirements of the Code.

DCCKI Authorised Subscribers

L13.2 Any Party or RDP may apply to become a DCCKI Authorised Subscriber in accordance with, and by following the relevant procedures set out in, the DCCKI Certificate Policy and the DCCKI RAPP.

L13.3 The DCC shall authorise any Party or RDP to submit a DCCKI Certificate Signing Request, or any User to submit a Personnel Authentication Certification Application, and so to become a DCCKI Subscriber, where that person has successfully completed the relevant procedures and satisfied the criteria set out in the DCCKI Certificate Policy and the DCCKI RAPP.

L13.4 The DCC shall provide any DCCKI Services that may be requested by a DCCKI Authorised Subscriber where the request is made by that DCCKI Authorised Subscriber in accordance with the applicable requirements of the DCCKI SEC Documents.

L13.5 The DCC shall ensure that in the provision of DCCKI Services it acts in accordance with Good Industry Practice.

Registration Data Providers

L13.6 Where a Registration Data Provider (other than an Electricity Network Party or Gas Network Party which is deemed to be an RDP, acting in its capacity as such) has become a DCCKI Authorised Subscriber, the Network Party that nominated that Registration Data Provider shall ensure that the RDP complies with all of its obligations in that capacity under this Section L13.

L13.7 Where a Registration Data Provider has been nominated as such by more than one Network Party:

(a) to the extent to which that RDP can be clearly identified as acting on behalf of one Network Party, that Network Party shall be subject to the requirements of Section L13.6 in respect of the actions of the RDP;

(b) to the extent to which that RDP cannot be clearly identified as acting on behalf of one Network Party, each of the Network Parties which nominated that RDP shall be subject to the requirements of Section L13.6 in respect of the actions of the RDP.

DCCKI Eligible Subscribers

L13.8 A DCCKI Authorised Subscriber:

(a) shall be known as a "**DCCKI Eligible Subscriber**" in respect of a DCCKI Certificate if it is entitled to become a DCCKI Subscriber for that DCCKI Certificate; and

(b) will be entitled to become a DCCKI Subscriber for a DCCKI Certificate only if it is identified as a DCCKI Eligible Subscriber in respect of that DCCKI Certificate in accordance with the provisions of the DCCKI Certificate Policy and the DCCKI RAPP.

DCCKI Subscribers

L13.9 A Party or RDP shall be entitled to become a DCCKI Subscriber in accordance with, and by following the relevant procedures set out in, the DCCKI Certificate Policy and the DCCKI RAPP.

The DCCKI Service Interface

DCC: Obligation to Maintain the DCCKI Service Interface

L13.10 The DCC shall maintain the DCCKI Service Interface in accordance with the DCCKI Interface Design Specification and make it available, to DCCKI Authorised Subscribers, for sending and receiving communications in accordance with the DCCKI Code of Connection.

L13.11 The DCC shall ensure that the DCCKI Service Interface is available at all times (subject to Planned Maintenance undertaken in accordance with Section H8.3):

(a) from the date on which the DCC is first obliged to provide the DCCKI Services in accordance with this Section L13; and

(b) prior to that date, on such dates and to such extent as is necessary for the purpose of facilitating Entry Process Testing.

The DCCKI Service Interface

L13.12 For the purposes of this Section L13, the “**DCCKI Service Interface**” means a communications interface designed to allow communications to be sent between a DCCKI Authorised Subscriber and the DCC for the purposes of the DCCKI Services.

DCCKI Interface Design Specification

L13.13 For the purposes of this Section L13, the “**DCCKI Interface Design Specification**” shall be a SEC Subsidiary Document of that name which:

(a) shall specify the technical details of the DCCKI Service Interface;

(b) shall include the protocols and technical standards that apply to the DCCKI Service Interface;

(c) shall base those technical standards on PKIX/IETF/PKCS open standards, where:

(i) PKIX is the Public Key Infrastructure for X.509 Certificates, being an IETF set of standards for certificate and certificate revocation list profiles as specified in IETF RFC 5280;

(ii) the IETF is the Internet Engineering Task Force; and

(iii) PKCS is the Public Key Cryptography Standard; and

(d) may set out the procedure by which a DCCKI Authorised Subscriber and the DCC may communicate over the DCCKI Service Interface, and may in particular specify any requirements on:

(i) a DCCKI Authorised Subscriber which accesses, or is seeking to access, the DCCKI Service Interface;

(ii) the DCC in relation to the provision of means of access to the DCCKI Service Interface and/or any steps which must be taken by it in relation to communications made by a DCCKI Authorised Subscriber and received by it over the DCCKI Service Interface.

DCCKI Code of Connection

L13.14 For the purposes of this Section L13, the "**DCCKI Code of Connection**" shall be a SEC Subsidiary Document of that name which:

(a) shall set out the way in which DCCKI Authorised Subscribers may access the DCCKI Service Interface;

(b) shall specify the procedure by which DCCKI Authorised Subscribers and the DCC may communicate over the DCCKI Service Interface;

(c) shall include a description of the way in which the mutual authentication and protection of communications taking place over the DCCKI Service Interface will operate; and

(d) may specify any requirements on a DCCKI Authorised Subscriber which accesses, or is seeking to access, the DCCKI Service.

DCCKI Interface Document Development

L13.15 The DCC shall develop drafts of the DCCKI Interface Design Specification and DCCKI Code of Connection:

(a) in accordance with the process set out at Section L13.16; and

(b) so that the drafts are available by no later than the commencement of Code Implementation SIT or 2 March 2015 (whichever is earlier), or such later date as may be specified by the Secretary of State.

L13.16 The process set out in this Section L13.16 for the development of drafts of the DCCKI Interface Design Specification and DCCKI Code of Connection is that:

(a) the DCC shall, in consultation with the Parties, RDPs and such other persons as it considers appropriate, produce a draft of each document;

(b) where a disagreement arises with any person who is consulted with regard to any proposal as to the content of either document, the DCC shall endeavour to reach an agreed proposal with that person consistent with the purposes of the document;

(c) the DCC shall send a draft of each document to the Secretary of State as soon as is practicable after it is produced, and shall when doing so provide to the Secretary of State:

(i) a statement of the reasons why the DCC considers that draft document to be fit for purpose; and

(ii) a summary of any disagreements that arose during consultation and that have not been resolved by reaching an agreed proposal; and

(d) the DCC shall comply with any requirements in a direction given to it by the Secretary of State in relation to either draft document, including in particular:

(i) any requirement to produce and submit to the Secretary of State a further draft of either document; and

(ii) any requirement as to the process to be followed by the DCC (and the time within which that process shall be completed) prior to submitting a further such draft.

The DCCKI Repository Service

The DCCKI Repository

L13.17 For the purposes of this Section L13, the “**DCCKI Repository**” means a System for storing and (subject to the provisions of this Section) making available copies of the following:

(a) all DCCKI Infrastructure Certificates;

(b) the Root DCCKICA Certificate and the EII DCCKICA Certificate;

(c) all versions of the DCCKI Certificate Policy;

(d) the latest version of the DCCKI RAPP;

(e) the latest version of the EII DCCKICA CRL;

(f) the latest version of the DCCKI ARL; and

(g) such other documents or information as the DCC, in its capacity as the provider of the DCCKI Services, may from time to time consider appropriate.

The DCCKI Repository Service

L13.18 The DCC shall establish, operate, maintain and make available the DCCKI Repository in accordance with the provisions of this Section L13 (the "**DCCKI Repository Service**").

L13.19 The DCC shall ensure that the documents and information described in Section L13.17 may be lodged in the DCCKI Repository by itself for the purpose of providing the DCCKI Services or complying with any other requirements placed on it under the Code.

L13.20 The DCC shall ensure that no person may lodge documents or information in the DCCKI Repository other than in accordance with Section L13.19.

L13.21 The DCC shall ensure that the DCCKI Repository may be accessed for the purpose of viewing and/or obtaining a copy of any document or information stored on it by any Party or RDP which reasonably requires such access in accordance, or for any purpose associated, with the Code.

L13.22 The DCC shall make available a copy of any document stored on the DCCKI Repository to the Panel or the SMKI PMA (or the Code Administrator acting on their behalf) following receipt of a reasonable request to do so.

Parties: Duties in relation to the DCCKI Repository

L13.23 No Party or RDP may access the DCCKI Repository for the purpose of viewing and/or obtaining a copy of any document or information stored on it except to the extent that it reasonably requires such access in accordance, or for any purpose associated, with the Code.

The DCCKI Repository Interface

DCC: Obligation to Maintain the DCCKI Repository Interface

L13.24 The DCC shall maintain the DCCKI Repository Interface in accordance with the DCCKI Repository Interface Design Specification and make it available to the Parties and to RDPs to send and receive communications in accordance with the DCCKI Repository Code of Connection and (where applicable) for the purpose of Entry Process Testing.

L13.25 The DCC shall ensure that the DCCKI Repository Interface is available at all times (subject to Planned Maintenance undertaken in accordance with Section H8.3):

(a) from the date on which the DCC is first obliged to provide the DCCKI Services in accordance with this Section L13; and

(b) prior to that date, on such dates and to such extent as is necessary for the purpose of facilitating Entry Process Testing.

The DCCKI Repository Interface

L13.26 For the purposes of this Section L13, the "**DCCKI Repository Interface**" means a communications interface designed to allow communications to be sent from and received by the DCCKI Repository for the purposes of the DCCKI Repository Service.

DCCKI Repository Interface Design Specification

L13.27 For the purposes of this Section L13, the "**DCCKI Repository Interface Design Specification**" shall be a SEC Subsidiary Document of that name which:

(a) specifies the technical details of the DCCKI Repository Interface; and

(b) includes the protocols and technical standards that apply to the DCCKI Repository Interface.

DCCKI Repository Code of Connection

L13.28 For the purposes of this Section L13, the "**DCCKI Repository Code of Connection**" shall be a SEC Subsidiary Document of that name which sets out the way in which the Parties and RDPs may access the DCCKI Repository Interface.

DCCKI Repository Interface Document Development

L13.29 The DCC shall develop drafts of the DCCKI Repository Interface Design Specification and DCCKI Repository Code of Connection:

(a) in accordance with the process set out at Section L13.30; and

(b) so that the drafts are available by no later than the commencement of Code Implementation SIT or 2 March 2015 (whichever is earlier), or such later date as may be specified by the Secretary of State.

L13.30 The process set out in this Section L13.30 for the development of drafts of the DCCKI Repository Interface Design Specification and DCCKI Repository Code of Connection is that:

(a) the DCC shall, in consultation with the Parties, RDPs and such other persons as it considers appropriate, produce a draft of each document;

(b) where a disagreement arises with any person who is consulted with regard to any proposal as to the content of either document, the DCC shall endeavour to reach an agreed proposal with that person consistent with the purposes of the document;

(c) the DCC shall send a draft of each document to the Secretary of State as soon as is practicable after it is produced, and shall when doing so provide to the Secretary of State:

(i) a statement of the reasons why the DCC considers that draft document to be fit for purpose; and

(ii) a summary of any disagreements that arose during consultation and that have not been resolved by reaching an agreed proposal; and

(d) the DCC shall comply with any requirements in a direction given to it by the Secretary of State in relation to either draft document, including in particular:

(i) any requirement to produce and submit to the Secretary of State a further draft of either document; and

(ii) any requirement as to the process to be followed by the DCC (and the time within which that process shall be completed) prior to submitting a further such draft.

The DCCKI Document Set

Obligations on the SMKI PMA

L13.31 The SMKI PMA shall exercise the functions that are allocated to it under and (in so far as they apply to it) comply with the requirements of the DCCKI Document Set.

Obligations on DCCKI Participants

L13.32 Each DCCKI Participant shall (in so far as they apply to it) comply with the requirements of the DCCKI SEC Documents.

The DCCKI Document Set

L13.33 For the purposes of this Section L13, the "**DCCKI Document Set**" means:

(a) the DCCKI SEC Documents; and

(b) the DCCKI CPS.

The DCCKI SEC Documents

L13.34 For the purposes of this Section L13, the "**DCCKI SEC Documents**" means the provisions of the Code comprising:

(a) the following SEC Subsidiary Documents:

(i) the DCCKI Certificate Policy;

(ii) the DCCKI RAPP;

(iii) the DCCKI Interface Design Specification;

(iv) the DCCKI Code of Connection;

(v) the DCCKI Repository Interface Design Specification;

(vi) the DCCKI Repository Code of Connection;

(b) the provisions of this Section L13; and

(c) every other provision of the Code which relates to the provision or the use of the DCCKI Services or the DCCKI Repository Service or to any matters directly arising from or affecting the provision or the use of those Services.

The DCCKI Registration Authority Policies and Procedures: Document Development

L13.35 The DCC shall develop a draft of the DCCKI RAPP:

(a) to make provision for such matters as are specified in the DCCKI Certificate Policy as being matters provided for in the DCCKI RAPP;

(b) to make provision for such other matters as are necessary or appropriate in relation to the exercise of its functions as the DCCKI Registration Authority;

(c) in accordance with the process set out at Section L13.36; and

(d) so that the draft is available by no later than the commencement of Code Implementation SIT or 2 March 2015 (whichever is earlier), or such later date as may be specified by the Secretary of State.

L13.36 The process set out in this Section L13.36 for the development of a draft of the DCCKI RAPP is that:

(a) the DCC shall, in consultation with the Parties, RDPs and such other persons as it considers appropriate, produce a draft of the DCCKI RAPP;

(b) where a disagreement arises with any person who is consulted with regard to any proposal as to the content of the DCCKI RAPP, the DCC shall endeavour to reach an agreed proposal with that person consistent with the purposes of the DCCKI RAPP specified in Section L13.35;

(c) the DCC shall send a draft of the DCCKI RAPP to the Secretary of State as soon as is practicable after it is produced, and shall when doing so provide to the Secretary of State:

(i) a statement of the reasons why the DCC considers that draft to be fit for purpose; and

(ii) a summary of any disagreements that arose during consultation and that have not been resolved by reaching an agreed proposal; and

(d) the DCC shall comply with any requirements in a direction given to it by the Secretary of State in relation to the draft of the DCCKI RAPP, including in particular:

(i) any requirement to produce and submit to the Secretary of State a further draft of the document; and

(ii) any requirement as to the process to be followed by the DCC (and the time within which that process shall be completed) prior to submitting a further such draft.

The DCCKI Certification Practice Statement

L13.37 The DCC shall establish, give effect to, maintain and comply with a document which shall be known as the "**DCCKI CPS**".

L13.38 The DCCKI CPS shall be a document which:

(a) sets out the policies and procedures of the DCC designed to ensure that it will comply with the requirements of the DCCKI Certificate Policy;

(b) incorporates the detailed operating procedures to be used by the DCC for the purposes of its compliance with the requirements of that Policy;

(c) incorporates such other provisions as may be required by or in accordance with that Policy or any other part of the Code;

(d) is reviewed by the SMKI PMA to assess whether it is appropriate for these purposes; and

(e) is approved by the individual(s) carrying out the DCCKI PMA Functions as being appropriate for these purposes.

L13.39 For the purposes of the review of the DCCKI CPS by the SMKI PMA in accordance with Section L13.38(d), the DCC shall submit an initial draft of the DCCKI CPS to the SMKI PMA by no later than the commencement of Code Implementation SIT or 2 March 2015 (whichever is earlier), or such later date as may be agreed by the SMKI PMA.

L13.40 The DCC shall keep the DCCKI CPS under review, and shall in particular carry out a review of the DCCKI CPS:

(a) whenever (and to the extent to which) it may be required to so by the SMKI PMA or the individual(s) carrying out the DCCKI PMA Functions; and

(b) following receipt of a notification from the SMKI PMA in accordance with Section L1.17(e) (Duties of the SMKI PMA).

L13.41 Following:

(a) any review of the DCCKI CPS, the DCC may propose amendments to it, which it shall submit to:

(i) the SMKI PMA for its review; and

(ii) the individual(s) carrying out the DCCKI PMA Functions for his (or their) approval;

(b) a review carried out in accordance with Section L13.40(b), the DCC shall report to the SMKI PMA any remedial steps taken or proposed to be taken in order for it to continue to meet its obligations under Section G (Security).

Enquiries in relation to the DCCKI Document Set

L13.42 The DCC shall respond within a reasonable time to any reasonable request for information made by a Party or RDP in relation to the DCCKI Services, the DCCKI Repository Service or the DCCKI Document Set, but excluding any request for a copy of any document or information which can be accessed through the DCCKI Repository.

The DCCKI Subscriber Obligations

DCCKI Certificate Signing Requests and Personnel Authentication Certificate Applications

L13.43 Each DCCKI Eligible Subscriber shall ensure that all of the information contained in each DCCKI Certificate Signing Request and each Personnel Authentication Certificate Application made by it is true and accurate.

L13.44 No DCCKI Eligible Subscriber may make a DCCKI Certificate Signing Request or Personnel Authentication Certificate Application which contains:

(a) any information that constitutes a trade mark, unless it is the holder of the Intellectual Property Rights in relation to that trade mark; or

(b) any confidential information which would be contained in a DCCKI Certificate Issued in response to that DCCKI Certificate Signing Request or Personnel Authentication Certificate Application.

Subscribing for or Rejecting DCCKI Certificates

L13.45 Where any DCCKI Certificate is Issued to a DCCKI Eligible Subscriber in response to a DCCKI Certificate Signing Request, or any Personnel Authentication Certificate is Issued to a DCCKI Eligible Subscriber in response to a Personnel Authentication Certificate Application, that DCCKI Eligible Subscriber shall:

(a) establish whether the information contained in that DCCKI Certificate or Personnel Authentication Certificate is consistent with information that was contained in the DCCKI Certificate Signing Request or Personnel Authentication Certificate Application (as the case may be);

(b) if it identifies that the DCCKI Certificate or Personnel Authentication Certificate contains any information which is untrue or inaccurate immediately inform the DCC that it rejects the DCCKI Certificate or Personnel Authentication Certificate and give to the DCC its reasons for doing so; and

(c) in the absence of any such rejection, become a DCCKI Subscriber for that DCCKI Certificate or Personnel Authentication Certificate.

Use of DCCKI Certificates

L13.46 Each DCCKI Subscriber shall ensure that it does not use any DCCKI Certificate held by it other than for the purposes of creating, sending, receiving and processing communications sent to and from the DCC pursuant to the Code.

DCCKI Certificates: Protection of Private Keys

L13.47 Each DCCKI Subscriber shall (in addition, if it is the DCC, a User or an RDP, to its obligations under Section G (Security)) take reasonable steps to ensure that no Compromise occurs to any:

(a) Private Key which is associated with a Public Key contained in a DCCKI Certificate for which it is the DCCKI Subscriber; or

(b) Secret Key Material associated with that Private Key.

The DCCKI Relying Party Obligations

DCCKI Relying Parties

L13.48 For the purposes of this Section L13, a "**DCCKI Relying Party**" in relation to a DCCKI Certificate or DCCKICA Certificate, means any Party or RDP which relies on the Certificate for the purposes of creating, sending, receiving or processing communications sent to and from the DCC or another Party or RDP pursuant to this Code.

Duties in relation to DCCKI Certificates and DCCKICA Certificates

L13.49 Each DCCKI Relying Party shall:

(a) before relying on any DCCKI Certificate:

(i) Check Cryptographic Protection in respect of the EII DCCKICA CRL (or, in the case of DCC only, any DCCKI Certificate Revocation List relevant to that DCCKI Certificate) on the DCCKI Repository, in accordance with IETF RFC 5280; and

(ii) where that DCCKI Certificate is shown on the EII DCCKICA CRL (or, in the case of DCC only, any DCCKI Certificate Revocation List relevant to that DCCKI Certificate) as having been revoked, not rely on the DCCKI Certificate; and

(b) before relying on any DCCKICA Certificate:

(i) Check Cryptographic Protection in respect of the DCCKI ARL on the DCCKI Repository, in accordance with IETF RFC 5280; and

(ii) where that DCCKICA Certificate is shown on the DCCKI ARL as having been revoked, not rely on the DCCKICA Certificate.

L13.50 No DCCKI Relying Party may rely on a DCCKI Certificate where the Validity Period of that DCCKI Certificate has expired.

L13.51 No DCCKI Relying Party may rely on a DCCKI Certificate or DCCKICA Certificate where it suspects that the DCCKI Certificate has been Compromised.

L13.52 Each DCCKI Relying Party shall take reasonable steps, by means of appropriate Systems, to verify Digital Signatures, Check Cryptographic Protection, Confirm Validity and perform other appropriate cryptographic operations before relying on any DCCKI Certificate or DCCKICA Certificate.

The DCCKI PMA Functions

Performance of the DCCKI Functions

L13.53 The DCC shall make arrangements which shall ensure that:

(a) a senior member of DCC Personnel;

(b) a senior member of the personnel of a DCC Service Provider; or

(c) a number of individuals, each of whom falls within either paragraph (a) or (b), acting together,

shall carry out the DCCKI PMA Functions. The DCCKI PMA Functions

L13.54 For the purpose of this Section L13, the "**DCCKI PMA Functions**" shall mean the activities of:

(a) approving the DCCKI CPS, and any amendments to it;

(b) periodically:

(i) reviewing the effectiveness of the DCCKI Document Set (including so as to evaluate whether the DCCKI Document Set remains consistent with the SEC Objectives); and

(ii) identifying any changes that should be made to the DCCKI Document Set in order to ensure that the DCC meets its obligations under Section G (Security);

(c) as soon as is reasonably practicable following the incorporation of each of the following documents into this Code, its re-incorporation, or its modification in accordance with section 88 of the Energy Act 2008, carrying out in relation to it the activities specified in paragraph (a) above:

(i) the DCCKI Certificate Policy;

(ii) the DCCKI RAPP;

(d) on receipt by the DCC of a notification from the SMKI PMA in accordance with Section L1.17(e) (Duties of the SMKI PMA), carrying out in relation to the DCCKI Document Set the activities specified in paragraph (a) above, having regard in particular to any recommendation for action made by the SMKI PMA; and

(e) performing any other duties expressly described as DCCKI PMA Functions elsewhere in this Code.

The Duties of the DCC

L13.55 Where the individual(s) carrying out the DCCKI PMA Functions notifies the DCC of any matter, or makes any recommendation with regard to the compliance by the DCC with its obligations under Section G (Security) (including in particular any recommendation for the modification of the DCCKI Document Set for the purpose of ensuring such compliance), the DCC shall:

(a) consider and take into account the matter notified, or recommendation made, to it; and

(b) where, having done so, it considers that it would be appropriate to make a change to the:

(i) DCCKI SEC Documents, submit a Draft Proposal for that purpose; and

(ii) DCCKI CPS, propose amendments to it in accordance with Section L13.42.

L13.56 The DCC shall ensure that the SMKI PMA and Security Sub-Committee shall each be provided with such of the following information as it may request:

(a) any notification or recommendation made to the DCC by the individual(s) carrying out the DCCKI PMA Functions; and

(b) copies of all agenda and supporting papers available at any meeting between individuals acting together to carry out the DCCKI PMA Functions, insofar as those agenda and papers are reasonably relevant to the functions of the SMKI PMA or Security Sub-Committee (as the case may be).

L13.57 The DCC shall ensure that, where it receives any report with regard to its ISO 27001 certification and part of that report relates to any matters concerned with the DCCKI Services, it will as soon as reasonably practicable provide those parts of that report to the SMKI PMA.

L14. THE S1SPKM DOCUMENT SET

Obligations on the SMKI PMA

L14.1 The SMKI PMA shall exercise the functions that are allocated to it under and (in so far as they apply to it) comply with the requirements of the S1SPKM Document Set.

Obligations on the DCC

L14.2 The DCC shall (in so far as they apply to it) comply with the requirements of the S1SPKM Document Set.

The S1SPKM Document Set

L14.3 For the purposes of this Section L14, the "**SMETS1 Service Provider Key Management Document Set**" (or "**S1SPKM Document Set**") means:

(a) the S1SPKM SEC Documents; and

(b) each S1SPKI CPS.

The S1SPKM SEC Documents

L14.4 For the purposes of this Section L14, the "**SMETS1 Service Provider Key Management SEC Documents** " (or "**S1SPKM SEC Documents**") means the provisions of the Code comprising:

(a) the following SEC Subsidiary Documents:

(i) each S1SPKI Certificate Policy;

(ii) each S1SPKI RAPP;

(iii) each SMETS1 Cryptographic Key Management Policy;

(iv) the SMKI Recovery Procedure;

(v) the S1SPKM Compliance Policy;

(b) the provisions of this Section L14; and

(c) every other provision of the Code which relates to the establishment, provision or use of any the S1SPKI, or to any matters directly arising from or affecting the establishment, provision or use of the S1SPKI.

The S1SPKI Certificate Policies: Document Development

L14.5 The DCC shall develop a draft of one or more S1SPKI Certificate Policies:

(a) so that each such S1SPKI CP shall be in equivalent form, and have content which corresponds, to the Organisation Certificate Policy; and

(b) in accordance with the process set out at Section L14.8.

The S1SPKI Registration Authority Policies and Procedures: Document Development

L14.6 The DCC shall develop a draft of one or more S1SPKI Registration Authority Policies and Procedures:

(a) so that there shall be an S1SPKI RAPP in respect of each S1SPKI CP;

(b) so that each such S1SPKI RAPP shall make provision for such matters as are specified in the related S1SPKI CP as being matters to be provided for in that S1SPKI RAPP;

(c) in accordance with the process set out at Section L14.8.

The SMETS1 Cryptographic Key Management Policy: Document Development

L14.7 The DCC shall, in respect of each SMETS1 Symmetric Key Arrangement, develop a draft of a SMETS1 Cryptographic Key Management Policy, which shall:

(a) be in accordance with the requirements of "A10.1.2 – Key Management" of ISO 27001;

(b) set out the policy on the use, protection and duration of the Symmetric Keys throughout their entire lifecycle;

(c) make provision for managing those Symmetric Keys throughout their entire lifecycle, including in particular provision for generating, storing, archiving, distributing, retiring and destroying them;

(d) specify secure procedures and methods for:

(i) generating Symmetric Keys for different cryptographic systems and different applications;

(ii) distributing Symmetric Keys to intended recipients;

(iii) activating the Symmetric Keys when received;

(iv) storing Symmetric Keys and providing access to them for authorised users;

(v) changing or updating Symmetric Keys, including provision for how and when they will be changed or updated;

(vi) dealing with Compromised Symmetric Keys;

(vii) revoking Symmetric Keys, including provision for how and when they are to be withdrawn or deactivated;

(viii) recovering Symmetric Keys that are lost or corrupted;

(ix) backing-up or archiving Symmetric Keys;

(x) destroying Symmetric Keys; and

(xi) the logging and auditing of key management related activities; and

(e) be developed in accordance with the process set out at Section L14.8.

Document Development: Process

L14.8 The process set out in this Section L14.8 for the development of a draft of any S1SPKI CP, S1SPKI RAPP and SMETS1 Cryptographic Key Management Policy, is that, in respect of each such document:

(a) the DCC shall, as soon as reasonably practicable after the coming into effect of this Section L14, in consultation with the Parties and such other persons as it considers appropriate, produce a draft of the document;

(b) where a disagreement arises with any person who is consulted with regard to any proposal as to the content of the document, the DCC shall endeavour to reach an agreed proposal with that person consistent with the purposes of the document specified in Section L14.5, L14.6 or L14.7 (as the case may be);

(c) the DCC shall send a draft of the document to the Secretary of State as soon as is practicable after it is produced, and shall when doing so provide to the Secretary of State:

(i) a statement of the reasons why the DCC considers that draft to be fit for purpose; and

(ii) a summary of any disagreements that arose during consultation, identifying in particular any that have not been resolved by reaching an agreed proposal; and

(d) the DCC shall comply with any requirements in a direction given to it by the Secretary of State in relation to the draft of the document, including in particular:

(i) any requirement to produce and submit to the Secretary of State a further draft of the document; and

(ii) any requirement as to the process to be followed by the DCC (and the time within which that process shall be completed) prior to submitting a further such draft.

The S1SPKI Certification Practice Statement

L14.9 The DCC shall establish, give effect to, maintain and comply with one or more documents, each of which shall be known as an "**S1SPKI Certification Practice Statement**" (or "**S1SPKI CPS**"), so that there shall be an S1SPKI CPS in respect of each S1SPKI CP

L14.10 Each S1SPKI CPS shall be a document which:

(a) sets out the policies and procedures of the DCC designed to ensure that it will comply with the requirements of the related S1SPKI Certificate Policy;

(b) incorporates the detailed operating procedures to be used by the DCC for the purposes of its compliance with the requirements of that Policy;

(c) incorporates such other provisions as may be required by or in accordance with that Policy or any other part of the Code; and

(d) has been reviewed by the SMKI PMA and either approved by it or not rejected (whether or not following the making of such amendments as may be directed by the SMKI PMA) in accordance with the provisions of Section L14.11(b).

L14.11 For the purposes of the review of an S1SPKI CPS by the SMKI PMA in accordance with Section L14.10(d):

(a) the DCC shall submit an initial draft of the document to the SMKI PMA as soon as reasonably practicable after the coming into effect of this Section L14;

(b) the SKMI PMA shall review the initial draft of the document and shall:

(i) approve the draft;

(ii) determine that the draft is not rejected;

(iii) reject the draft; or

(iv) notify the DCC that it will either approve the draft or the determine that the draft is not rejected subject to the DCC first making such amendments to the document as it may direct; and

(c) the DCC shall make any amendments to the draft document that may be directed by the SMKI PMA in accordance with sub-paragraph (b)(iv).

L14.12 The DCC shall keep each S1SPKI CPS under review, and shall in particular carry out a review of an S1SPKI CPS:

(a) whenever (and to the extent to which) it may be required to so by the SMKI PMA; and

(b) following receipt of a notification from the SMKI PMA in accordance with Section L1.17(q) (Duties of the SMKI PMA).

L14.13 Following:

(a) any review of an S1SPKI CPS, the DCC may propose amendments to that document, and:

(i) any such amendments shall be submitted by the DCC to the SMKI PMA for its review; and

(ii) following the review by the SMKI PMA, the provisions of Sections L14.11(b) and (c) shall apply in respect of those amendments as they applied to the initial draft of the S1SPKI CPS; and

(b) a review carried out in accordance with Section L14.12(b), the DCC shall report to the SMKI PMA any remedial steps taken or proposed to be taken in order for it to continue to meet its obligations under Section G (Security).

L15. S1SPKM ASSURANCE

S1SPKM Compliance Policy

L15.1 The SKMI PMA shall exercise the functions allocated to it by the S1SPKM Compliance Policy.

L15.2 The DCC shall procure all such services as are required for the purposes of complying with its obligations under the S1SPKM Compliance Policy.

The DCC: Duty to Cooperate in Assessment

L15.3 The DCC shall do all such things as may be reasonably requested by the SMKI PMA, or by any person acting on behalf of or at the request of the SMKI PMA (including in particular the Independent S1SPKM Assurance Service Provider), for the purposes of facilitating an assessment of the DCC's compliance with any applicable requirements of the S1SPKM Document Set.

L15.4 For the purposes of Section L15.3, the DCC shall provide the SMKI PMA (or the relevant person acting on its behalf or at its request) with:

(a) all such Data as may reasonably be requested, within such times and in such format as may reasonably be specified; and

(b) all such other forms of cooperation as may reasonably be requested, including in particular access at all reasonable times to:

(i) such parts of the premises of the DCC as are used for; and

(ii) such DCC Personnel as carry out, or are authorised to carry out,

any activities related to its compliance with the applicable requirements of the S1SPKM Document Set.

Events of Default

L15.5 In relation to an Event of Default which consists of a material breach by the DCC of any applicable requirements of the S1SPKM Document Set, the provisions of Sections M8.2 (Notification of an Event of Default) to M8.4 (Consequences of an Event of Default) shall apply subject to the provisions of Sections L15.6 to L15.12.

L15.6 For the purposes of Sections M8.2 to M8.4 as they apply pursuant to Section L15.5, an Event of Default shall (notwithstanding the ordinary definition thereof) be deemed to have occurred in respect of the DCC where it is in material breach of any applicable requirements of the S1SPKM Document Set (provided that Sections M8.4(e), (f) and (g) shall never apply to the DCC).

L15.7 Where in accordance with Section M8.2 the Panel receives notification that the DCC is in material breach of any applicable requirements of the S1SPKM Document Set, it shall refer the matter to the SMKI PMA. On any such referral, the SMKI PMA may investigate the matter in accordance with Section M8.3 as if the references in that Section to the "Panel" were to the "SMKI PMA".

L15.8 Where the SMKI PMA has:

(a) carried out an investigation in accordance with Section M8.3; or

(b) received a report from the Independent S1SPKM Assurance Service Provider, following an assessment by it of the compliance of the DCC with the applicable requirements of the S1SPKM Document Set, concluding that the DCC has not complied with those requirements,

the SMKI PMA shall consider the information available to it and shall determine whether any non-compliance with the SMKI Document Set has occurred and, if so, whether that non-compliance constitutes an Event of Default.

L15.9 Where the SMKI PMA determines that an Event of Default has occurred, it shall:

(a) notify the DCC and any other Party it considers may have been affected by the Event of Default; and

(b) refer the matter to the Panel for the Panel to determine the appropriate steps to take in accordance with Section M8.4.

L15.10 Where the Panel is considering what steps to take in accordance with Section M8.4, it shall request and consider the advice of the SMKI PMA.

L15.11 Where the Panel determines that the DCC is required to give effect to a remedial action plan in accordance with Section M8.4(d) that plan must be approved by the SMKI PMA.

L15.12 Where, in accordance with Section L15.11, the SMKI PMA has approved a remedial action plan in relation to the DCC, the Panel may arrange for a version of the approved plan (or parts of that plan) to be made available to all the Parties, but only where the Panel considers that such dissemination is necessary for the purposes of security.

L16. SUPPLIER OF LAST RESORT

L16.1 Where the Authority notifies the DCC of a Failing Energy Supplier, the DCC shall notify the SMKI PMA, and the following shall apply:

(a) the DCC shall not revoke the Supplier Certificates of the Failing Energy Supplier until the DCC is directed to do so by the SMKI PMA;

(b) subject to consideration of the circumstances in Section L16.2, the SMKI PMA shall promptly:

(i) direct the DCC to immediately revoke one or more of the Supplier Certificates; and/or

(ii) notify the DCC of the SMKI PMA’s decision not to direct the immediate revocation of one or more of the Supplier Certificates; and

(c) the SMKI PMA shall notify the Authority of the SMKI PMA’s decision under Section L16.1(b).

L16.2 For the purposes of Section L16.1(b), the SMKI PMA shall (to the extent that the information is available to them) take into account the following:

(a) the fact that the Failing Energy Supplier will cease to be an Eligible Subscriber and/or DCCKI Eligible Subscriber for the Supplier Certificates when its Gas Supply Licence and/or Electricity Supply Licence is revoked;

(b) the arrangements in place under the Customer Supply Continuity Plan(s) of the Failing Energy Supplier;

(c) whether there is a Shared Resource Provider which provides (or provided) Shared Resources to the Failing Energy Supplier, and (if so):

(i) the ability of the Shared Resource Provider to send Service Requests and/or to amend Anomaly Detection Thresholds using the Private Keys associated with Public Keys in the Failing Energy Supplier's Supplier Certificates; and

(ii) whether the staff who operated the Failing Energy Supplier’s User Systems have been (or are likely to be) retained by the Supplier of Last Resort;

(d) whether the Failing Energy Supplier has (or had) any Pre-Payment Consumers;

(e) any adverse impact on the Energy Consumers of the Failing Energy Supplier that may arise from any decision made by the SMKI PMA to direct the revocation of one or more of the Supplier Certificates of the Failing Energy Supplier, including that this adverse impact might be exacerbated by the fact that there is likely to be a period of time between the appointment of the Supplier of Last Resort and the completion of the SoLR Change of Supplier Processes; and

(f) any other matters that the SMKI PMA considers relevant in the circumstances of the case.

L16.3 Where, in the case of a Failing Energy Supplier, the SMKI PMA notifies the Authority of the SMKI PMA's intention to not direct the immediate revocation of one or more of the Supplier Certificates, the Authority may direct a Shared Resource Provider for the Failing Energy Supplier to take action to maintain continuity of the physical supply of gas and/or electricity to the Pre-Payment Consumers of the Failing Energy Supplier.

L16.4 Where directed by the Authority under Section L16.3, the Shared Resource Provider shall expeditiously take the steps (if any) that are practically available to it to maintain continuity of the supply of gas and/or electricity to the Pre-Payment Consumers of the Failing Energy Supplier.

L16.5 It is acknowledged that:

(a) in order to meet its obligation under Section L16.4, a Shared Resource Provider may use the Private Keys associated with Public Keys contained within the Supplier Certificates of the Failing Energy Supplier in order to:

(i) submit Service Requests to the DCC that result in the sending of Commands to SMETS2+ Devices or to a SMETS1 Service Provider; and/or

(ii) modify the Anomaly Detection Thresholds in order to allow it to meet its obligation in a timely manner;

(b) in order to meet its obligation under Section L16.4 to take steps expeditiously, the Shared Resource Provider may need also to communicate with Smart Metering Systems which do not include Smart Meters operating as Pre-Payment Meters;

(c) the effect of the actions of the Shared Resource Provider may result in one or more of the Pre-Payment Consumers of the Failing Energy Supplier continuing to receive a physical supply of gas and/or electricity notwithstanding that no advance payment has been made for that supply; and

(d) the actions of the Shared Resource Provider may be taken before or after the Supplier of Last Resort is Registered as supplier to the Pre-Payment Consumers of the Failing Energy Supplier.

L16.6 Each Supplier of Last Resort shall, as soon as reasonably practicable after it is appointed as Supplier of Last Resort in relation to a Failing Energy Supplier, notify the SMKI PMA that the Supplier of Last Resort wishes the Shared Resource Provider to either:

(a) cease to use the Failing Energy Supplier's Private Keys in accordance with Section L16.4; or

(b) continue to use the Failing Energy Supplier's Private Keys in accordance with Section L16.4 for a period of time, and hence that Supplier of Last Resort does not wish the SMKI PMA to direct the DCC to revoke the Supplier Certificates of the Failing Energy Supplier that have not yet been revoked, in which case the Supplier of Last Resort shall:

(i) give details to the SMKI PMA to justify why the Supplier of Last Resort believes this is necessary;

(ii) set out its plans to complete the SoLR Change of Supplier Processes in relation to relevant Devices, including the timetable within which it expects this process to be completed; and

(iii) update the SMKI PMA on a weekly basis (or more regularly where requested by the SMKI PMA).

L16.7 Following a notification from the relevant Supplier of Last Resort pursuant to Section L16.6, the SMKI PMA shall consider whether or not to direct the DCC to revoke any or all of the Failing Energy Supplier's Supplier Certificates (by reference to the matters in Section L16.2). This is without prejudice to the authority of the SMKI PMA to, at any time, direct the DCC to revoke any or all of the Failing Energy Supplier's Supplier Certificates.

L16.8 Each of the Failing Energy Supplier and the Supplier of Last Resort hereby waives any and all claims it might otherwise have had against the Shared Resource Provider in respect of the steps taken by the Shared Resource Provider in compliance with Section L16.4.

L16.9 Where the SMKI PMA directs the DCC not to revoke one or more of the Failing Energy Supplier's Supplier Certificates, the SMKI PMA shall also direct the DCC not to recognise the transfer of the Failing Energy Supplier's Market Participant Identifiers to the Supplier of Last Resort, where this will assist in enabling the Shared Resource Provider to take steps required by this Section L16.1. The DCC shall comply with each such direction until the SMKI PMA or the Authority directs otherwise.

L17. INTERACTIONS WITH CSS

L17.1 The DCC shall use a Private Key associated with a Public Key that is contained within an Organisation Certificate to Digitally Sign any communication sent pursuant to Section E2.19.

Annex A to Section L

Table 1: Remote Party Roles and associated Remote Party Role Codes in addition to those specified in the GB Companion Specification

Remote Party Role	Remote Party Role Code
pPPXmlSign	128
pPRDPFileSign	129
s1SPxmlSigning	126
commissioningPartyFileSigning	132
requestingPartyFileSigning	131
s1SPMigrationSigning	130
commissioningPartyXmlSigning	133
cSSProvider	134
xmlSign	135
coSPartyXmlSign	136
dSPXmlSign	137
aCBXmlSign	138
wANProviderXmlSign	139

M GENERAL

M1. COMMENCEMENT AND DURATION

Commencement

M1.1 This Code shall take effect from the effective date designated by the Secretary of State pursuant to Condition 22 of the DCC Licence.

Duration

M1.2 Once this Code comes into effect, it shall remain in effect:

(a) in respect of the DCC, until the DCC ceases to be a Party in accordance with Section M9 (Transfer of the DCC Licence); and

(b) in respect of each Party other than the DCC, until (subject to Section M8.14) such Party ceases to be a Party in accordance with Section M8 (Suspension, Expulsion and Withdrawal).

M2. LIMITATIONS OF LIABILITY

Unlimited Liabilities

M2.1 Nothing in this Code or any Bilateral Agreement shall exclude or limit a Party's Liability:

(a) for death or personal injury resulting from the negligence of that Party;

(b) for fraud or fraudulent misrepresentation;

(c) to pay the Charges and any interest accruing in respect of the Charges in accordance with this Code; or

(d) for any other type of Liability which cannot by law be excluded or limited.

Exclusion of Indirect Loss

M2.2 No Party shall in any circumstances be liable to another Party for loss arising as a result of a breach of this Code and/or any Bilateral Agreement that does not directly result from such breach and that was not reasonably foreseeable as likely to occur in the ordinary course of events.

Confidentiality and Intellectual Property Rights

M2.3 Each Party's Liability for breaches of Section M4 (Confidentiality) shall be:

(a) in the case of any breach of Section M4.20 (Confidentiality of DCC Data) relating to Data that has been clearly by the DCC as 'confidential', unlimited (save as provided in Section M2.2); and

(b) in the case of any other breach of Section M4, limited to £1,000,000 (one million pounds) in respect of each incident or series of related incidents, save as provided in Section M2.3A).

M2.3A The Liability of the DCC for a breach of Section M4.1 (Prohibition on disclosure and use by DCC) shall, where the amount of that Liability is recoverable by the DCC from a DCC Service Provider in accordance with the terms of a DCC Service Provider Contract, be:

(a) unlimited if the amount of the Liability that is recoverable from the DCC Service Provider is unlimited; or

(b) limited to any amount in which the Liability that is recoverable from the DCC Service Provider is limited, or to £1,000,000 (one million pounds) in respect of each incident or series of related incidents, whichever is the greater,

but, for the purposes of this Section, no regard shall be had to any limitation in a DCC Service Provider Contract which is expressed to be set by reference to any amount specified in or calculated under this Code.

M2.4 Each Party’s Liability for any breach of Section M5 (Intellectual Property Rights) shall be unlimited (save as provided in Section M2.2).

Damage to Physical Property

M2.5 Subject to Section M2.1, each Party’s Liability for loss of or damage to physical property (including loss of or damage to Systems, and loss or corruption of Data) arising as a result of a breach by that Party of this Code and/or any Bilateral Agreement shall be limited as follows:

(a) the Liability of the DCC shall be limited to £1,000,000 (one million pounds) in respect of each incident or series of related incidents; and

(b) the Liability of each Party other than the DCC shall be limited to £1,000,000 (one million pounds) in respect of each incident or series of related incidents,

for which purposes:

(c) where a defect in the design, manufacture, materials or workmanship of two (or more) Devices causes loss of or damage to physical property (including loss of or damage to Systems, and loss or corruption of Data), the defect in each such Device shall constitute a separate unrelated incident; and

(d) where a Party's Liability exceeds £1,000,000 (one million pounds) and is limited under this Section M2.5 and that Liability is in respect of loss or damage suffered by more than one other Party, each such other Party shall be entitled to recover a proportion of the £1,000,000 (one million pounds) calculated by reference to the amount of any loss and damage suffered by it expressed as a fraction of the total amount of loss and damage suffered by such other Parties collectively.

Recovery of Loss which is Expressly Permitted

M2.6 It is expressly agreed that a Party may recover the following losses arising as a result of a breach of this Code (and without intending to limit recovery of any other Liability that may arise as a result of such breach):

(a) (subject to Sections F9.25 (Exclusive Remedies for Site Visits) and M2.5) where such breach causes the loss of, or damage to, a Smart Metering System (or any part of it), the Import Supplier, Export Supplier and/or Gas Supplier (as applicable) for that Smart Metering System shall be entitled to recover the reasonable costs and expenses (including reasonable labour costs) incurred in attending the relevant premises for the purpose of repairing or replacing that Smart Metering System (or the relevant part of it);

(b) in the case of breaches of Section F6 (Delivery and Acceptance of Communications Hubs) and/or the CH Handover Support Materials, the DCC shall be entitled to recover the reasonable costs and expenses referred to in Section F6.18 (Failure to Accept Delivery);

(c) where such breach causes an Organisation Certificate to be Compromised or issued otherwise than in accordance with the relevant Certificate Policy (and, in either case, the Subscriber wishes it to be replaced), the reasonable costs and expenses (including reasonable labour costs) incurred in replacing any or all such Compromised Certificates held on Devices (but not the costs and expenses of replacing Device Certificates), limited to £1,000,000 (one million pounds) in respect of each incident or series of related incidents); and

(d) where such breach (including a breach which is deemed to occur in accordance with Section L10.26 (Breach of the Code by the Relevant Subscriber)) gives rise to a Recovery Event such that the DCC incurs (or is required to make payments in respect of) Recovery Costs under Section L10 (the SMKI Recovery Procedure), the DCC shall be entitled to recover the Recovery Costs that it has incurred (or been required so to pay), limited to £1,000,000 (one million pounds) in respect of each Recovery Event.

Exclusion of Loss of Profit etc.

M2.7 Subject to Sections M2.1 and M2.6 and save in the case of a breach referred to in Section M2.3(b) or M2.4, no Party shall in any circumstances be liable to another Party for any of the following losses arising as a result of a breach of this Code and/or any Bilateral Agreement:

(a) loss of profit;

(b) loss of revenue;

(c) loss of use;

(d) loss of contract;

(e) loss of goodwill; or

(f) loss resulting from the liability of such other Party to a third party for any of the matters referred to in paragraphs (a) to (e) above.

Exclusion of Other Liabilities

M2.8 Subject to Sections M2.1 and M2.6 and save in the case of a breach of those provisions referred to in Section M2.3 or M2.4, no Party shall be liable to any other Party for loss arising from any breach of this Code and/or any Bilateral Agreement other than for losses that are subject to Section M2.5. This Section M2.8 is without prejudice to the operation of the Charging Methodology, and the payments required under Section F9.22 (Payment of Type Fault and Batch Fault Compensation) or F9.23 (Compensation for Product Recall or Technology Refresh).

M2.9 The rights and remedies provided by this Code and/or any Bilateral Agreement are exclusive and not cumulative, and exclude and are in place of all substantive (but not procedural) rights or remedies provided by common law or statute in respect of the subject matter of this Code and/or any Bilateral Agreement, including any rights that any Party may possess in tort (or delict).

M2.10 Subject to Section M2.1, each of the Parties hereby waives to the fullest extent possible all such rights and remedies provided by common law or statute (and releases the other Parties to the same extent from all Liabilities or obligations provided by common law or statute in respect of the subject matter of this Code and/or any Bilateral Agreement).

Statutory Rights

M2.11 For the avoidance of doubt, nothing in this Section M2 shall exclude or restrict or otherwise prejudice or affect any of:

(a) the rights, powers, duties and obligations of any Party which are conferred or created by the Relevant Instruments; or

(b) the rights, powers and duties of the Authority or the Secretary of State.

Other Matters

M2.12 Each of the sub-clauses of this Section M2 shall be construed as a separate and severable contract term, and if one or more of such sub-clauses is held to be invalid, unlawful or otherwise unenforceable, then the other or others of such sub-clauses shall remain in full force and effect and shall continue to bind the Parties.

M2.13 In respect of all substantive (but not procedural) rights or remedies provided by common law or statute (including in tort or delict, but without prejudice to contractual rights or remedies) in respect of loss of or damage to physical property (including loss of or damage to Systems, and loss or corruption of Data) arising in relation to the subject matter of this Code and/or any Bilateral Agreement, it is agreed that:

(a) each Party hereby waives and releases (to the fullest extent possible at law) such rights and remedies in respect of such loss or damage as such Party may otherwise have against the contractors, employees and agents of each other Party (including the DCC Service Providers) in their capacity as such;

(b) the DCC shall ensure that each DCC Service Provider (when acting in its capacity as such) waives and releases (to the fullest extent possible at law) such rights and remedies in respect of such loss or damage as such DCC Service Provider may otherwise have against the Parties other than DCC in their capacity as such (and/or against the contractors, employees and agents of such Parties in their capacity as such);

(c) the waiver and release referred to in Section M2.13(a) is to be enforceable by the persons stated therein to have the benefit thereof in accordance with Section M11.5 (Third Party Rights); and

(d) the DCC shall ensure that the waiver and release referred to in Section M2.13(b) is enforceable by the persons stated therein to have the benefit thereof under the Contracts (Rights of Third Parties) Act 1999.

M2.14 Each Party shall be under a duty to mitigate its loss.

M2.15 Each Party hereby acknowledges and agrees that the provisions of this Section M2 are fair and reasonable having regard to the circumstances.

Conduct of Indemnity Claims

M2.16 Where this Code provides that one Party (the "Indemnifier") is to indemnify another Party (the "Indemnified Party") against third party claims, the Indemnified Party shall:

(a) promptly notify the Indemnifier of any such claim, and provide it with details in relation to the same and all relevant documentation excluding that which attracts legal privilege;

(b) consult with the Indemnifier with respect to the subject matter of the claim and the manner in which the Indemnified Party intends to deal with the same, keep the Indemnifier promptly advised of developments concerning the same, and have due regard to the Indemnifier's views in relation to the same;

(c) not settle, compromise or make any admission of liability concerning any such claim, without the prior written consent of the Indemnifier (such consent not to be unreasonably withheld or delayed); and

(d) where the Indemnifier so requests, allow the Indemnifier (or such person as the Indemnifier may nominate) to conduct all negotiations and proceedings regarding the claim (at the Indemnifier's cost), in which case the Indemnifier shall ensure that the claim is diligently defended in accordance with any reasonable instructions of the Indemnified Party and not settled or compromised without the Indemnified Party's consent (such consent not to be unreasonably withheld or delayed).

SECCo

M2.17 The provisions of this Section M2 (and the definitions used in this Section) shall apply to SECCo as if SECCo was a Party, but shall not limit SECCo's liability under Section C3.12 (Protections for Panel Members and Others).

M2.18 Nothing in this Section M2 shall limit the DCC's liability to reimburse SECCo in respect of Recoverable Costs.

M3. SERVICES FM AND FORCE MAJEURE

Force Majeure affecting the Services - Services FM

M3.1 The concept of Services FM applies in respect of the obligations of the DCC to provide the Services pursuant to this Code (including pursuant to any Bilateral Agreement).

M3.1A The concept of Services FM is in addition to the concept of OPR Exceptional Events which applies under and in accordance with Sections H13.7 to H13.14 (OPR Exceptional Events). It is possible for an event or circumstance to constitute both an OPR Exceptional Event and Services FM, in which case the DCC may seek relief under both Sections H13.7 to H13.14 (OPR Exceptional Events) and this Section M3. Notwithstanding any other provision of this Section M3, relief for the purposes of OPR Reporting will only arise under and in accordance with the process for OPR Exceptional Events in Sections H13.7 to H13.14 (OPR Exceptional Events).

M3.2 The DCC may claim relief from Liability for non-performance of its obligations in respect of the Services to the extent this is due to Services FM. To the extent that performance of the DCC's obligations is unaffected by the Services FM, the provisions of this Code and any Bilateral Agreement will continue to apply.

M3.3 The DCC cannot claim Services FM has occurred:

(a) in relation to any wilful act, neglect or failure to take reasonable precautions against the relevant Services FM event by the DCC or its servants, agents, employees or contractors (including the DCC Service Providers);

(b) in relation to any circumstances resulting from a failure or delay by any other person in the performance of that other person's obligations under a contract with the DCC other than this Code (unless that other person is itself prevented from or delayed in complying with its obligations as a result of Services FM); and/or

(c) as a result of any shortage of labour, material or other resources unless caused by circumstances which are themselves Services FM, and in any event, the DCC shall not be entitled to relief if and to the extent that it is required to comply with the BCDR Procedure in accordance with Sections H10.9 and H10.10 (the Business Continuity and Disaster Recovery Procedure) but has failed to do so (unless this failure is also due to Services FM affecting the operation of the BCDR Procedure).

M3.4 The DCC shall, as soon as reasonably practicable (and in any event within five (5) days of the occurrence of the Services FM), give to the Users that were due to receive the affected Services and to the Panel full details of the Services FM and any relief the DCC wishes to claim in connection with the Services FM.

M3.5 The DCC shall be entitled to relief in respect of Services FM to the extent that the Panel agrees following consultation with any relevant Sub-Committee (or it is subsequently determined by arbitration) that the requirements of Sections M3.2 and M3.3 are met, and that:

(a) the DCC could not have avoided the occurrence of the Services FM (or its consequences or likely consequences) by taking steps which the DCC was required to take (or procure) under this Code and any Bilateral Agreement or might reasonably be expected to have taken;

(b) the Services FM directly caused the non-performance of the Services for which relief is claimed;

(c) the time lost and/or relief from the obligations under this Code and any Bilateral Agreement claimed by the DCC could not reasonably be expected to be mitigated or recovered by the DCC acting in accordance with Good Industry Practice; and

(d) the DCC is taking all steps in accordance with Good Industry Practice to overcome or minimise the consequences of the Services FM on the performance of the Services.

M3.5A The Panel shall reach a determination as to whether the DCC is entitled to relief in respect of Services FM in accordance with Section M3.5 within 10 Working Days after the DCC notifies the Panel of the Services FM under Section M3.4.

M3.6 If the DCC is entitled to relief in respect of Services FM in accordance with Section M3.5, then:

(a) the DCC shall be relieved of Liability under this Code and any Bilateral Agreement in respect of the Services to the extent to which that Liability would otherwise have arisen solely as a result of the Services FM; and

(b) for the avoidance of doubt, the Charges (but not, for the avoidance of doubt, the Fixed Charges) payable by a User shall be reduced to the extent that the DCC does not provide the Services to that User as a result of the Services FM (and shall be calculated on the basis of the Services that are actually provided).

M3.7 The DCC shall notify the affected Users and the Panel as soon as reasonably practicable after the Services FM ceases or no longer causes the DCC to be unable to comply with its obligations under this Code and/or any Bilateral Agreement in respect of the Services. Following such notification, the Services shall continue to be performed in accordance with the terms and conditions existing immediately before the occurrence of the Services FM.

M3.8 The DCC hereby irrevocably and unconditionally waives all and any rights to claim any extension or allowance of time or other relief from performance of its obligations in respect of the Services other than to the extent caused by Services FM (but without prejudice to the process applying to OPR Exceptional Events. Each User hereby irrevocably and unconditionally waives all and any rights to claim compensation (including for breach of contract or in tort) for failure by the DCC to provide the Services to the extent caused by Services FM.

Force Majeure

M3.9 The concept of Force Majeure applies in respect of:

(a) all obligations of the DCC pursuant to this Code and any Bilateral Agreement other than the obligations of the DCC to provide the Services; and

(b) all obligations of the other Parties pursuant to this Code and any Bilateral Agreement,

all such obligations together being in this Section M3 the "**Relevant Obligations**". For clarity, OPR Exceptional Events (which are defined by reference to Force Majeure) also apply in respect of the DCC claiming relief in respect of its obligations to provide the Services for the purposes of OPR Reporting under Sections H13.7 to H13.14 (OPR Exceptional Events).

M3.10 Subject to Section M3.11, the Affected Party will not be in breach of this Code and/or any Bilateral Agreement or otherwise liable for any failure or delay in performance of any Relevant Obligations to the extent such failure or delay is caused by Force Majeure.

M3.11 An Affected Party may only rely upon Section M3.10 in respect of a failure or delay in performance of any Relevant Obligations to the extent that the Affected Party and the Party or Parties to whom the Affected Party owes the Relevant Obligations agree (or it is determined by arbitration) that the Affected Party:

(a) notified the Party or Parties to whom the Affected Party owes those Relevant Obligations of the matters constituting Force Majeure as soon as reasonably practicable following their occurrence;

(b) kept such Party or Parties fully informed as to the matters relating to the Force Majeure; and

(c) took all reasonable steps in accordance with Good Industry Practice to overcome the Force Majeure and/or minimise the consequences of the Force Majeure on the performance of the Relevant Obligations.

M3.12 The Affected Party shall notify the Party or Parties to whom the Affected Party owes the Relevant Obligations as soon as reasonably practicable after the Force Majeure ceases or no longer causes the Affected Party to be unable to comply with the Relevant Obligations.

M3.13 Each Party hereby irrevocably and unconditionally waives all and any rights to claim any extension or allowance of time or other relief from performance of the Relevant Obligations other than to the extent caused by Force Majeure. Each Party hereby irrevocably and unconditionally waives all and any rights to claim compensation (including for breach of contract or in tort) for, or to seek to expel the Affected Party from this Code for, any failure by the Affected Party to comply with the Relevant Obligations to the extent caused by Force Majeure.

SECCo

M3.14 The provisions of this Section M3 (and the definitions used in this Section) shall apply to SECCo as if SECCo was a Party.

M4. CONFIDENTIALITY

Prohibition on disclosure and use by DCC

M4.1 Subject to Sections M4.3 and M4.4, the DCC shall not disclose another Party's Confidential Information to, or authorise access to another Party's Confidential Information by, any person.

M4.2 Subject to Section M4.3, the DCC shall not use a Party's Confidential Information for any purpose other than the purpose for which it was provided (or otherwise made available) to the DCC, and in any event for any purpose other than the purposes of this Code

Circumstances in which disclosure or use by the DCC are permitted

M4.3 The restrictions on disclosure and authorisation of access in Section M4.1 and on use in Section M4.2 shall not apply to the disclosure or use of, or authorisation of access to, a Party's Confidential Information to the extent:

(a) expressly permitted or required by the DCC Licence;

(b) necessary for the exercise by the DCC of any of its obligations under the Electricity Act, the Gas Act, the DCC Licence, or this Code;

(c) made or given in accordance with the Authority's prior written consent;

(d) such Confidential Information is already available in the public domain other than as a result of a breach by the DCC of this Section M4 and/or the DCC Licence; or

(e) such Confidential Information is already lawfully in the possession of the DCC otherwise than as a result (whether directly or indirectly) of a breach of this Code and/or the DCC Licence (but without prejudice to any obligations to which the DCC is subject in respect of the use or disclosure of such Confidential Information under the arrangements relating to such lawful possession).

M4.4 The restrictions on disclosure and authorisation of access in Section M4.1 shall not apply to the disclosure of, or authorisation of access to, a Party's Confidential Information to the extent:

(a) made or given in order to comply with the DCC's duties under Laws and Directives or the rules of any recognised stock exchange; provided that, in so far as is reasonably practicable in accordance with such Laws and Directives or rules, the DCC shall provide that Party with prior notice of such proposed disclosure or authorisation of access; or

(b) made or given to the employees, other agents, contractors or advisers of the DCC to the extent such persons require such Confidential Information for the purpose of performing their roles as such; provided that such persons are subject to restrictions on the disclosure or use of, or authorisation of access to, such Confidential Information equivalent to those under this Section M4, and provided that the DCC shall be liable for any disclosure, authorisation or use by such persons otherwise than in accordance with this Section M4. This Section M4.4(b) is without prejudice to Section M4.5.

Restriction of disclosure to DCC employees who are leaving

M4.5 The DCC shall not (having regard to the nature and effective life of the Confidential Information in question) continue to disclose Confidential Information to (or authorise access to Confidential Information by) an employee or other agent of the DCC who has notified DCC of his or her intention to become engaged as an employee or agent of:

(a) any other Party; or

(b) a broker or consultant who is known to provide services in relation to the Supply of Energy and/or Commercial Activities,

save where the DCC could not, in all the circumstances, reasonably be expected to refrain from divulging to such employee or other agent Confidential Information which is required for the proper performance of his or her duties.

DCC Practices, Systems and Procedures

M4.6 The DCC shall put in place and at all times maintain managerial and operational practices, systems, and procedures designed to ensure that it complies with this Section M4.

Provision of Information to the Panel

M4.7 Each Party agrees, subject to any confidentiality provision binding on it, to provide to the Panel (or its Sub-Committees and/or Working Groups, including via the Code Administrator, the Secretariat or SECCo) all Data reasonably requested by the Panel (or its Sub-Committees and/or Working Groups, including via the Code Administrator, the Secretariat or SECCo) in order that they may properly carry out their duties and functions under this Code.

Confidentiality and the Panel

M4.8 Where a Party wishes its Party Data to remain confidential, it shall:

(a) in the case of the DCC (in so far as it acts in accordance with Sections M4.22 to M4.24), clearly mark such Party Data as either 'confidential' or 'controlled'; and

(b) in the case of any other Party, clearly mark such Party Data as 'confidential'.

M4.9 Where a Party does not clearly mark its Party Data as ’confidential’, or (in the case of the DCC only)'controlled', the Panel (or its Sub-Committees or Working Groups, the Code Administrator, the

Secretariat or SECCo, as applicable) may treat such Party Data as not being confidential (and shall have no confidentiality obligation in respect of the same).

M4.10 Subject to Section M4.11, the Panel shall not (and shall also ensure that its Sub- Committees and Working Groups, the Code Administrator, the Secretariat and SECCo shall not) disclose, or authorise access to, any Party Data provided (or otherwise made available) to them by a Party where that Party has clearly marked such Party Data as 'confidential' or (in the case of the DCC only) 'controlled' in accordance with Section M4.8.

M4.11 The restrictions in Section M4.10 on disclosures of, or authorisation of access to, Party Data shall not apply to the extent:

(a) made or given in accordance with duties under Laws and Directives or instructions of the Authority;

(b) such Party Data is already available in the public domain other than as a result of a breach by the Panel (or its Sub-Committees or Working Groups, the Code Administrator, the Secretariat or SECCo); or

(c) such Party Data is already lawfully in the possession of the Panel (or its Sub- Committees or Working Groups, the Code Administrator, the Secretariat or SECCo) otherwise than as a result (whether directly or indirectly) of this Code and/or the DCC Licence (but without prejudice to any obligations in respect of the use or disclosure of such Party Data under the arrangements relating to such lawful possession).

M4.12 The Parties acknowledge that, in order for the Panel (and its Sub-Committees and Working Groups, the Code Administrator, the Secretariat and SECCo) to properly carry out their duties and functions under this Code, the Panel may decide (or be obliged) to keep Data as confidential, and not disclose that Data to the Parties. The Panel shall take reasonable steps to keep such instances to a minimum.

Panel Information Policy

M4.13 The Panel shall establish and maintain a policy for classifying, labelling, handling and storing Party Data received by it (and its Sub-Committees and Working Groups, the Code Administrator, the Secretariat and SECCo) pursuant to the provisions of Section G (Security), Section I (Data Privacy), and Section L (Smart Metering Key Infrastructure) and its related SEC Subsidiary Documents.

M4.14 The Panel (and its Sub-Committees and Working Groups, the Code Administrator, the Secretariat and SECCo) shall act in accordance with the policy established and maintained in accordance with Section M4.13.

Confidentiality of DCC Data

M4.15 Where Data belonging to the DCC, or relating to the DCC or the Services, is disclosed (or otherwise becomes available) to another Party under or in relation to this Code, and where the DCC wishes such Data to remain confidential, the DCC shall (in so far as it acts in accordance with Sections M4.22 to M4.24) clearly mark such Data as either 'confidential' or 'controlled' and where the DCC does not do so, the other Parties may treat such Data as not being confidential (and shall have no confidentiality obligation in respect of the same).

M4.16 Where a Party wishes to dispute whether or not Data which the DCC has marked as 'controlled' may be given that designation in accordance with Section M4.23, that Party may refer the matter to arbitration in accordance with Section M7 (Dispute Resolution).

M4.17 Where a Party wishes to be able to receive from the DCC Data which the DCC marks as 'confidential', that Party shall:

(a) provide to the DCC a list containing the names and contact details of one or more individuals who are authorised by it to receive such Data; and

(b) where it wishes to change the names and/or contact details of the individuals on the list, provide an updated version of the list to the DCC a reasonable time in advance of the update taking effect.

M4.18 Where a Party has provided to the DCC in accordance with Section M4.17 the names and contact details of one or more individuals who are authorised by it to receive Data marked by the DCC as 'confidential', the DCC shall not disclose such Data to that Party except by sending it or making it available to all of those named individuals.

M4.19 Where a Party has not provided to the DCC the names and contact details of one or more individuals who are authorised by it to receive Data marked by the DCC as 'confidential':

(a) the DCC shall be under no obligation to, and shall not, disclose any such Data to that Party; and

(b) paragraph (a) shall be deemed to take precedence over any contrary provision of this Code, and any such provision shall be read as if it incorporated no requirement to disclose any Data marked by the DCC as 'confidential'.

M4.20 Each Party other than the DCC shall not disclose, or authorise access to, Data that is clearly marked by the DCC as either 'confidential' or 'controlled', in accordance with Section M4.15, provided that such restrictions on disclosure and access shall not apply to the extent that:

(a) the disclosure is made or given in accordance with duties under Laws and Directives or instructions of the Authority;

(b) such Data is already available in the public domain other than as a result of a breach of this Code by a Party;

(c) such Data is already lawfully in the possession of the Party otherwise than as a result (whether directly or indirectly) of this Code and/or the DCC Licence (but without prejudice to any obligations in respect of the use or disclosure of such Data under the arrangements relating to such lawful possession); or

(d) such Data is clearly marked by the DCC as 'confidential', but the DCC has disclosed it to the Party by sending or making it available to an individual not named in a list provided by the Party under Section M4.17, or by using contact details different to those specified in that list, and:

(i) the disclosure or access occurs as a direct consequence of that breach by the DCC of Section M4.18; and

(ii) if the Party was made or otherwise became aware of that breach by the DCC, it had taken all reasonable steps to avoid the disclosure or access.

Use of DCC Data

M4.21 The Parties other than the DCC may only use the Data belonging to the DCC, or relating to the DCC or the Services, which is disclosed (or otherwise becomes available) to them under or in relation to this Code for the purpose of performing their obligations or exercising their rights under this Code (or for any other use that is expressly authorised by the DCC in writing).

DCC Classification of Data

M4.22 For the purposes of Sections M4.8 and M4.15, the DCC may only mark Data as 'confidential' where:

(a) that Data relates to a DCC Service Provider providing services pursuant to a DCC Service Provider Contract which was referred to in paragraph 1.5 of schedule 1 to the DCC Licence on its grant;

(b) the DCC is subject to an existing obligation under the DCC Service Provider Contract referred to in paragraph (a) to ensure that that Data remains confidential;

(c) the DCC's Liability for breaching the obligation referred to in paragraph (b) is unlimited; and

(d) the DCC is not prohibited from marking that Data as 'confidential' under Section M4.24.

M4.23 For the purposes of Sections M4.8 and M4.15, the DCC may only mark Data as 'controlled' where:

(a) the uncontrolled disclosure of, or uncontrolled authorised access to, that Data could reasonably be considered to be prejudicial to the DCC (or any DCC Service Provider); and

(b) the DCC is not prohibited from marking that Data as 'controlled' under Section M4.24.

M4.24 The DCC shall not mark Data as either 'confidential' or 'controlled' where or to the extent that:

(a) the DCC is expressly required to place that Data in the public domain in order to comply with its duties under Laws and Directives;

(b) it is necessary for the exercise by the DCC of any of its obligations under the Electricity Act, the Gas Act, the DCC Licence, or this Code to place that Data in the public domain; or

(c) that Data is already in the public domain other than as a result of a breach by the Parties or the Panel of this Section M4 and/or the DCC Licence.

Onward Supply of Supplier Party Data

M4.25 Where the DCC is obliged under a condition of the DCC Licence to disclose to a third party for a specified purpose information relating to a Supplier Party, that Supplier Party shall, where requested to do so, consent to the further disclosure of that information by that third party to the extent such further disclosure is necessary to fulfil that specified purpose.

Injunctive Relief

M4.26 The Parties agree that damages may not be an adequate remedy in the event of breach of this Section M4, and that a Party may seek injunctive relief in respect of any breach or potential breach of this Section M4.

M5. INTELLECTUAL PROPERTY RIGHTS

SEC Materials

M5.1 Section M5.2 applies in respect of this Code and any and all documents, materials, reports, charts and tables, diagrams and specifications, and any and all other works, inventions, ideas, designs or proposals (in whatever form, and including Draft Proposals and Modification Proposals) arising out of or in connection with the central administration, operation and development of this Code, including any and all associated drafts and working papers (collectively, the "**SEC Materials**"); provided that the SEC Materials shall not include the Consumer Data or the Services IPR.

M5.2 The Parties agree that, as between the Parties, any and all Intellectual Property Rights subsisting in the SEC Materials and the whole of the title to the SEC Materials will:

(a) be owned by SECCo; and

(b) automatically and immediately vest in SECCo upon their creation or acquisition.

M5.3 Where a Party other than SECCo acquires (by operation of Laws and Directives or otherwise) any Intellectual Property Rights in the SEC Materials, then that Party:

(a) (as far as is permitted by law) hereby assigns such Intellectual Property Rights to SECCo with full title guarantee, by way of present assignment of future Intellectual Property Rights; and

(b) (to the extent such assignment is not permitted) shall (and shall procure that any of its employees, agents or contractors shall) do all acts and things and execute all documents that may be reasonably necessary to transfer such Intellectual Property Rights to SECCo with full title guarantee (and pending such assignment shall hold such rights on trust for SECCo).

M5.4 SECCo hereby grants to each of the other Parties (for so long as they remain a Party) a royalty-free, non-exclusive, non-transferable licence to use the SEC Materials for the sole purpose of participating as a Party (including exercising its rights and performing its obligations as a Party). Each licence granted to a Party under this Section M5.4 includes the right of that Party to grant sub-licences to its agents, contractors and advisers provided that they are granted solely in respect of that Party's participation as a Party (and the SEC Materials are used for no other purpose).

M5.5 SECCo hereby grants to each of the Panel Members, any Sub-Committee or Working Group members, the Code Administrator and the Secretariat (for so long as they each remain such) a royalty-free, non-exclusive, non-transferable licence to use the SEC Materials for the sole purpose of performing their roles as such. Each licence granted to a person under this Section M5.5 includes the right of that person to grant sub- licences to its agents, contractors and advisers provided that they are granted solely in respect of that person's performance of the role for which the licence was granted (and the SEC Materials are used for no other purpose).

Consumer Data

M5.6 Section M5.7 applies in respect of the Data that is obtained by the DCC (or its employees, other agents or contractors) as a result of providing Services to that User, including the Data contained in requests for Services and that is obtained as a result of communicating with Smart Metering Systems pursuant to this Code on behalf of a User (such Data being the "**Consumer Data**" of that User).

M5.7 As between the DCC and each User, any and all Intellectual Property Rights subsisting in the Consumer Data of that User shall be owned by that User (and the DCC shall make no claims in respect of such Intellectual Property Rights).

M5.8 Each User, in respect of its Consumer Data, hereby grants to the DCC a royalty-free, non-exclusive, non-transferable licence to use that Consumer Data for the sole purpose of DCC exercising its rights and performing its obligations under the Electricity Act, the Gas Act, the DCC Licence and this Code. Each licence granted to the DCC under this Section M5.8 includes the right of the DCC to grant sub-licences to its agents, contractors and advisers provided that they are granted solely in respect of the DCC's rights and obligations under the Electricity Act, the Gas Act, the DCC Licence and this Code (and the Consumer Data is used for no other purpose).

M5.9 Each User, in respect of its Consumer Data, shall ensure that the DCC (and its agents, contractors and advisers) can use that Consumer Data in the manner envisaged by Section M5.8, and shall indemnify the DCC in respect of any Liabilities suffered or incurred by the DCC (or its agents, contractors or advisers) as a result of claims brought by persons alleging that the use of that Consumer Data in the manner envisaged by Section M5.8 has infringed any Intellectual Property Rights.

Party Data

M5.10 Section M5.11 applies in respect of the Data (other than SEC Materials and Consumer Data) that is provided (or otherwise made available) pursuant to this Code to the Panel (or its Sub-Committees and/or Working Groups, including via the Code Administrator, the Secretariat or SECCo) by or on behalf of a Party (such Data being the "**Party Data**" of that Party).

M5.11 As between the Panel (including its Sub-Committees and/or Working Groups, the Code Administrator, the Secretariat and SECCo) and each Party, any and all Intellectual Property Rights subsisting in the Party Data of that Party shall be owned by that Party (and none of the Panel, its Sub-Committees, its Working Groups, the Code Administrator, the Secretariat or SECCo shall make any claims in respect of such Intellectual Property Rights).

M5.12 Without prejudice to Section M4.10 (Confidentiality and the Panel), each Party, in respect of its Party Data, hereby grants to SECCo, the Panel Members, any Sub- Committee or Working Group members, the Code Administrator and the Secretariat a royalty-free, non-exclusive, non-transferable licence to use that Party Data for the sole purpose of performing their roles as such. Each licence granted to a person under this Section M5.12 includes the right of that person to grant sub-licences to its agents, contractors and advisers provided that they are granted solely in respect of that person's performance of the role for which the licence was granted (and the Party Data is used for no other purpose).

M5.13 Without prejudice to Section M4.10, each Party, in respect of its Party Data, shall ensure that SECCo, the Panel Members, any Sub-Committee or Working Group members, the Code Administrator and the Secretariat (and their agents, contractors and advisers) can use that Party Data in the manner envisaged by Section M5.12, and shall indemnify the SECCo, the Panel Members, any Sub-Committee or Working Group members, the Code Administrator and the Secretariat in respect of any Liabilities suffered or incurred by them (or their agents, contractors or advisers) as a result of claims brought by persons alleging that the use of that Party Data in the manner envisaged by Section M5.12 has infringed any Intellectual Property Rights.

Services IPR

M5.14 Section M5.15 applies in respect of the Intellectual Property Rights created by, arising from or that are associated with:

(a) the activities undertaken by the DCC for the purposes of carrying on its Authorised Business (as defined in the DCC Licence) in accordance with the DCC Licence; or

(b) the operation of a DCC Service Provider Contract in accordance with its provisions,

such Intellectual Property Rights being the "**Services IPR**".

M5.15 As between the DCC and each User, the Services IPR shall be owned by the DCC (and no User shall make any claims in respect of the Services IPR).

M5.16 The DCC hereby grants to each User a royalty-free, non-exclusive, non-transferable licence to use the Services IPR for the sole purpose of receiving (and to the extent necessary to receive) the Services. Each licence granted by the DCC under this Section M5.16 includes the right of the User to grant sub-licences to its agents, and contractors provided that they are granted solely for the purpose of the User receiving (and to the extent necessary for the User to receive) the Services (and that the Services IPR is used for no other purpose).

M5.17 The DCC shall ensure that each User (and its agents and contractors) can use the Services IPR in the manner envisaged by Section M5.16, and shall indemnify each User in respect of any Liabilities suffered or incurred by that User (or its agents or contractors) as a result of claims brought by persons alleging that the use of that Services IPR in the manner envisaged by Section M5.16 has infringed any Intellectual Property Rights.

General

M5.18 For the avoidance of doubt, the use by a Party of Intellectual Property Rights licensed to it under this Section M5 otherwise than in accordance with such licence shall constitute a breach of this Code.

M5.19 The Parties agree that damages may not be an adequate remedy in the event of breach of this Section M5, and that a Party may seek injunctive relief in respect of any breach or potential breach of this Section M5.

SECCo

M5.20 The provisions of this Section M5 (and the definitions used in this Section) shall apply to SECCo as if SECCo was a Party.

M6. PARTY DETAILS

Provision of the Party Details

M6.1 Each Party's original Party Details shall be provided as part of its Framework Agreement counterpart or its Accession Agreement (as applicable).

Amendments to Party Details

M6.2 Each Party may amend its Party Details by notice to the Secretariat from time to time, and each Party shall ensure that its Party Details remain up-to-date.

Publication

M6.3 The Secretariat shall maintain a record of each Party's Party Details, and shall publish that record on the Website (other than those elements of the Party Details that are identified in Schedule 5 as being confidential).

M6.4 As soon as reasonably practicable after each person becomes a Party, or following notification of an amendment to a Party's Party Details in accordance with Section M6.2, the Secretariat shall update the record referred to in Section M6.3.

M6.5 The Secretariat shall take reasonable steps to identify any errors or omissions in each Party's Party Details, and shall notify the relevant Party of any such errors or omissions.

M7. DISPUTE RESOLUTION

Duty to Seek to Resolve

M7.1 Where a Dispute arises between two or more Parties, each such Party shall seek to resolve the Dispute amicably within a reasonable timescale through negotiation in good faith.

Reference to the Authority

M7.2 Any Dispute of a nature that is expressly stated in this Code or in the Electricity Act or the Gas Act or in the Energy Licences to be subject to determination by the Authority shall be subject to determination by the Authority (which shall be final and binding for the purposes of this Code). For the purposes of Condition 20.3(c) of the DCC Licence, disputes of the nature referred to in Condition 20 of the DCC Licence in respect of the following Other Enabling Services shall be subject to determination by the Authority pursuant to that condition:

(a) requests by TCH Participants for Test Communications Hubs pursuant to Section F10 Test Communications Hubs);

(b) requests by Parties for Detailed Evaluations pursuant to Section H7.7 (Detailed Evaluations of Elective Communication Services);

(c) requests by Parties for the provision of further assistance in respect of the Parse and Correlate Software pursuant to Section H11.12 (Provision of Support and Assistance to Users);

(d) requests by Testing Participants for the provision of a connection to a simulation of the SM WAN for the purposes of testing pursuant to Section H14.31 (Device and User System Tests);

(e) requests by Testing Participants for the provision of additional testing support pursuant to Section H14.33 (Device and User System Tests); and

(f) requests by Parties for DCC Gateway Connections pursuant to Section H15 (DCC Gateway Connections).

Reference to the Panel or its Sub-Committees

M7.3 Any Dispute of a nature that is expressly stated in this Code or a Bilateral Agreement to be subject to determination by the Panel (or one of its Sub-Committees) shall be subject to determination by the Panel (or that Sub-Committee). The Panel shall ensure that any such Dispute is determined within a reasonable period of time after its referral to the Panel (or its Sub-Committee).

M7.4 Unless such determination by the Panel (or one of its Sub-Committees) is expressly stated in this Code or a Bilateral Agreement to be final and binding, such disputes shall (following the Panel's or Sub-Committee's determination) be subject to final determination by the Authority (where this is expressly stated to be the case) or as referred to in Section M7.5.

Arbitration

M7.5 Subject to Sections M7.2, M7.3 and M7.4, any Dispute shall be subject to determination by arbitration in accordance with Section M7.6 (subject to Section M7.13).

M7.6 Where this Section M7.6 applies:

(a) the Party seeking to initiate the arbitration shall give a written notice to the other Party or Parties involved in the Dispute, stating that the matter is to be referred to arbitration and setting out a brief summary of the Dispute;

(b) the Party seeking to initiate the arbitration shall send a copy of that notice to the Panel;

(c) to the extent consistent with this Section M7.6, the arbitration shall be subject to the Arbitration Act 1996 and the rules of the London Court of International Arbitration (the LCIA);

(d) the arbitrator shall be a person appointed by agreement between the Parties involved in the Dispute, or (in the absence of agreement within 10 Working Days following the notice under Section M7.6(a)) appointed by the LCIA;

(e) (unless otherwise agreed by the Parties involved in the Dispute) the arbitration proceedings shall take place in London and in the English language;

(f) the Parties involved in the Dispute agree to keep the arbitration process (and the decision or anything said, done or produced in or in relation to the arbitration process) confidential, except as may be required by Laws and Directives and provided that representatives of the Panel may attend the arbitration and receive a copy of the decision;

(g) the Panel shall treat the decision and all other information relating to the arbitration as confidential, and Section M4.10 (Confidentiality and the Panel) shall apply to the decision and such information;

(h) the arbitrator shall have the power to make provisional awards as provided for in Section 39 of the Arbitration Act 1996; and

(i) subject to any contrary award by the arbitrator, each Party involved in the Dispute shall bear its own costs in relation to the arbitration and an equal share of the fees and expenses of the arbitrator.

M7.7 The decision of the arbitrator pursuant to a reference in accordance with Section M7.6 shall be final and binding on each of the Parties to the arbitration, except where there is a serious irregularity (as defined in section 68(2) of the Arbitration Act 1996) or a Party successfully appeals the arbitral award on a point of law in accordance with section 69 of the Arbitration Act 1996. Each Party shall comply with such decision provided that (for the avoidance of doubt) the arbitrator shall not have the power to modify this Code.

DCC Service Provider Disputes

M7.8 If any Dispute that is subject to determination by arbitration involves the DCC, and the DCC considers that the Dispute relates to a dispute it has under or in relation to one or more of the DCC Service Provider Contracts, then the DCC may join the relevant DCC Service Provider or DCC Service Providers to the arbitration, so that the arbitrator hears and determines the disputes under or in relation to the DCC Service Provider Contracts simultaneously with the Dispute. The Parties other than the DCC hereby consent to such joining of disputes.

M7.9 Where the DCC is aware of any dispute arising under or in relation to one or more DCC Service Provider Contracts that may reasonably relate to a Dispute or potential Dispute that would be subject to arbitration, then the DCC may give notice of that dispute to the Panel and to any or all of the other Parties.

M7.10 Where the DCC gives notice to a Party under Section M7.9, such notice shall only be valid if the DCC gives reasonable detail of such dispute and expressly refers to the waiver that may potentially be given by that Party under Section M7.12.

M7.11 Within 30 Working Days after the DCC has given a valid notification to a Party under Section M7.9 in respect of a dispute under or in relation to a DCC Service Provider Contract, that Party should give notice to the DCC of any Dispute that that Party wishes to bring in relation to that dispute. Where that Dispute is to be resolved by arbitration, the DCC may then exercise its rights under Section M7.8.

M7.12 Where the DCC gives notice to a Party in accordance with Section M7.9, and where that Party does not give notice to the DCC in accordance with Section M7.11, then that Party shall be deemed to have waived any right it may have to bring a claim against the DCC in respect of the subject matter of the dispute in question (and shall, notwithstanding Section M2 (Limitations of Liability), indemnify the DCC in full against any Liabilities incurred by the DCC as a consequence of that Party bringing any such claim).

Claims by Third Parties

M7.13 Subject to Section M7.14, if any person who is not a Party to this Code brings any legal proceedings in any court against any Party and that Party considers such legal proceedings to raise or involve issues that are or would be the subject matter of a Dispute or potential Dispute that would (but for this Section M7.13) be subject to arbitration, then (in lieu of arbitration) the court in which the legal proceedings have been commenced shall hear and determine the legal proceedings and the Dispute between such person and the Parties.

M7.14 If any person who is not a Party to this Code brings any legal proceedings in any court against any Party and that Party considers such legal proceedings to raise or involve issues that are the subject matter of a Dispute that is already subject to an ongoing arbitration, then Section M7.13 shall only apply where the arbitrator in that arbitration determines that such legal proceedings raise or involve issues that are the subject matter of the Dispute.

Injunctive Relief

M7.15 Nothing in this Section M7 shall prevent a Party seeking interim or interlocutory remedies in any court in relation to any breach of this Code.

SECCo

M7.16 The provisions of this Section M7 (and the definitions used in this Section) shall apply to SECCo as if SECCo was a Party.

M8. SUSPENSION, EXPULSION AND WITHDRAWAL

Events of Default

M8.1 An "**Event of Default**" shall have occurred in respect of any Party other than the DCC (the "**Defaulting Party**") if one or more of the following occurs in respect of the Defaulting Party:

(a) the Defaulting Party has committed a material breach of Section I1.2 (User Obligations);

(b) the Defaulting Party has failed in a material respect to comply with an enforcement notice served by the Information Commissioner pursuant to the Data Protection Legislation, whether such failure has been notified to the Panel by the Information Commissioner or the Panel has otherwise become aware of such failure;

(c) the DCC has served a notice on the Defaulting Party in accordance with Section J2.1 (Notification of Payment Failure) in respect of Charges payable by the Defaulting Party, and such Charges have not been paid within three (3) Working Days following that notice;

(d) the DCC has issued a notice to the Defaulting Party in accordance with Section J3.14 (Breach of Credit Cover Obligations) in respect of Credit Support required to be procured by the Defaulting Party, and such Credit Support has not been provided within three (3) Working Days following that notice;

(e) the Defaulting Party has not paid any amount other than in respect of the Charges (failures in respect of which are subject to Section M8.1(c)) which the Defaulting Party is due to have paid under this Code, and does not remedy such failure within five (5) Working Days after a notice requiring it to do so (which notice must refer to this Section M8);

(f) the Defaulting Party has made a material misrepresentation in its Application Form;

(g) the Defaulting Party is in material breach of any of its material obligations under this Code and/or any Bilateral Agreement (other than those that are subject to another paragraph of this Section M8.1) and the Defaulting Party has failed to remedy the breach (or to desist from the breach and mitigate its effects insofar as it is reasonably practicable to do so) within 20 Working Days after a notice requiring it to do so (which notice must describe the breach in reasonable detail and refer to this Section M8); and/or

(h) the Defaulting Party suffers an Insolvency Type Event.

Notification of an Event of Default

M8.2 Where the DCC or the Code Administrator or the Secretariat becomes aware that an Event of Default has occurred in respect of a Party, then the DCC or the Code Administrator or the Secretariat (as applicable) shall notify the Panel of such occurrence. Where any Party other than the DCC becomes aware that an Event of Default has occurred in respect of another Party, the Party that has become so aware may notify the Panel of such occurrence.

Investigation of an Event of Default

M8.3 Where the Panel has reason to believe that an Event of Default may have occurred in respect of a Party, then the Panel may investigate the circumstances relating to such potential Event of Default. Each Party shall provide all reasonable Data and cooperation as the Panel may reasonably request in respect of any such investigation.

Consequences of an Event of Default

M8.4 Where an Event of Default occurs in respect of a Defaulting Party and while that Event of Default is continuing, the Panel may take one or more of the following steps (in each case to the extent and at such time as the Panel sees fit, having regard to all the circumstances of the Event of Default and any representations made by any Competent Authority or any Party, provided that the Panel must always take the steps referred to in Section M8.4(a) and (b)):

(a) notify the Authority that such Event of Default has occurred in respect of the Defaulting Party;

(b) notify the Defaulting Party that such Event of Default has occurred in respect of it;

(c) notify each other Party that such Event of Default has occurred in respect of the Defaulting Party;

(d) require the Defaulting Party to give effect to a reasonable remedial action plan designed to remedy and/or mitigate the effects of the Event of Default within a reasonable timescale (a material breach of which plan shall in itself constitute an Event of Default);

(e) suspend one or more of the Defaulting Party's rights referred to in Section M8.5 (following such prior consultation with the Defaulting Party as the Panel considers appropriate);

(f) instruct the DCC to suspend (in which case the DCC shall, within one Working Day thereafter, suspend) one or more of the Defaulting Party's rights referred to in Section M8.6 (following such prior consultation with the Defaulting Party as the Panel considers appropriate); and/or

(g) expel the Defaulting Party from this Code subject to and in accordance with Section M8.10.

Suspension of Rights

M8.5 The rights referred to in Section M8.4(e) are:

(a) the right of the Defaulting Party (and each other member of its Voting Group) to vote in Panel Member elections under Section C4 (Panel Elections);

(b) the right of the Defaulting Party to raise new Draft Proposals under Section D (Modifications); and

(c) the right of the Defaulting Party to influence the appointment of a Change Board Member, so that:

(i) in the case of a Supplier Party, the Change Board Member appointed by the Voting Group of which that Supplier Party forms part shall be suspended; or

(ii) in the case of any Party other than a Supplier Party, the Secretariat shall ignore the views of that Party when considering any request to appoint or remove a Change Board Member appointed by the Party Category of which that Party forms part.

M8.6 The rights referred to in Section M8.4(f) are:

(a) the right of the Defaulting Party to receive Core Communication Services or Local Command Services in the ‘Other User’ User Role;

(b) (subject to the Authority's approval) the right of the Defaulting Party to receive Core Communication Services or Local Command Services in any User Role other than the 'Other User' User Role;

(c) (subject to the Authority’s approval) the right of the Defaulting Party to receive any or all Elective Communication Services;

(d) (subject to the Authority’s approval) the right of the Defaulting Party to initiate Enrolment of Smart Metering Systems; and

(e) (subject to the Authority’s approval) the right of the Defaulting Party to request or receive any or all Services other than those referred to elsewhere in this Section M8.6.

M8.7 The suspension of any or all of the Defaulting Party’s rights referred to in Section M8.5 or M8.6 shall be without prejudice to the Defaulting Party’s obligations and Liabilities under and in relation to this Code (whether accruing prior to, during, or after such suspension). Without prejudice to the generality of the foregoing, the Defaulting Party shall continue to be liable for all Charges that it is or becomes liable to pay under this Code.

M8.8 Where the Panel has, pursuant to Section M8.4(e) and/or (f), suspended a Party’s rights, then the Panel may at any time thereafter end such suspension (provided that, in the case of rights that the Panel cannot suspend without the Authority’s approval, the Panel may not end such suspension without the Authority’s approval).

Ceasing to be a Party

M8.9 A Party that holds an Energy Licence that requires that Party to be a party to this Code:

(a) cannot be expelled from this Code by the Panel unless the Authority has approved such expulsion (and, in the case of any such approval, Section M8.10(a) shall apply as if the Party did not hold an Energy Licence that requires it to be a party to this Code); and

(b) cannot voluntarily cease to be a Party while that Energy Licence remains in force.

M8.10 A Party that does not hold an Energy Licence that requires that Party to be a party to this Code:

(a) may (while an Event of Default is continuing in respect of that Party) be expelled from this Code with effect from such time on such date as the Panel may resolve (where the Panel considers it reasonable to do so in the circumstances); and

(b) may give notice to the Panel of that Party's intention to voluntarily cease to be a Party and of the time on the date from which it wishes to cease to be a Party. The Panel shall, following receipt of such a notice, resolve that that Party shall cease to be a Party with effect from the time on the date notified.

M8.11 The Panel shall notify the Authority and each remaining Party in the event that any person is expelled from this Code or voluntarily ceases to be a Party.

Appeal to the Authority

M8.12 Where the Panel resolves to suspend the rights of a Party and/or to expel a Party pursuant to this Section M, then that Party may at any subsequent time apply to the Authority to have such suspension lifted or to be reinstated as a Party. The Parties and the Panel shall give effect to any decision of the Authority pursuant to such application, which shall be final and binding for the purposes of this Code.

Consequences of Ceasing to be a Party

M8.13 Where the Panel makes a resolution in respect of a Party in accordance with Section M8.10, then with effect from the time on the date at which such resolutions are effective:

(a) that Party's accession to this Code shall be terminated, and it shall cease to be a Party; and

(b) subject to Section M8.14, that Party shall cease to have any rights or obligations under this Code or any Bilateral Agreement.

M8.14 The termination of a Party's accession to this Code shall be without prejudice to:

(a) those rights and obligations under this Code and/or any Bilateral Agreement that may have accrued prior to such termination; or

(b) those provisions of this Code or any Bilateral Agreement that are expressly or by implication intended to survive such termination, including Sections A (Definitions and Interpretation), J (Charges), L16 (Supplier of Last Resort), M2 (Limitations of Liability), M5 (Intellectual Property Rights), M7 (Dispute Resolution), M10 (Notices), and M11 (Miscellaneous).

M9. TRANSFER OF DCC LICENCE

Introduction

M9.1 This Section M9 is included in accordance with Condition 22 of the DCC Licence, and provides for the transfer of (amongst other things) the DCC's interest in this Code to a Successor Licensee.

Application and Interpretation of this Section M9

M9.2 This Section M9 shall only apply where two persons hold a DCC Licence at the same time. In such circumstances:

(a) "Transfer Date" has the meaning given to that expression in Condition 43 of the earlier of the two DCC Licences;

(b) until the Transfer Date, the holder of the earlier DCC Licence shall be "the DCC" for the purposes of this Code, and the holder of the later DCC Licence shall be "the Successor Licensee"; and

(c) from the Transfer Date, all references in this Code to "the DCC" shall be references to the holder of the later DCC Licence.

Novation Agreement

M9.3 Where this Section M9 applies, the DCC and the Successor Licensee shall each enter into a novation agreement in a form approved by the Authority.

M9.4 Such novation agreement will, with effect from the Transfer Date, novate to the Successor Licensee all rights and obligations of the DCC under the agreements referred to in Section M9.5 (including all rights obligations and liabilities of the DCC that may have accrued in respect of the period prior to the Transfer Date).

M9.5 Such novation agreement shall be in respect of the following agreements:

(a) the Framework Agreement;

(b) all Accession Agreements; and

(c) all Bilateral Agreements.

M9.6 The DCC shall enter into such novation agreement in (to the extent applicable) its own right, and also (to the extent applicable) on behalf of the Parties (which shall include SECCo) that are counterparties to the agreements referred to in Section M9.5.

DCC Authority to enter into Accession Agreements

M9.7 Each Party (which shall include SECCo) hereby irrevocably and unconditionally authorises the DCC to execute and deliver, on behalf of such Party, a novation agreement as envisaged by this Section M9.

Co-operation

M9.8 Each Party shall do all such things as the Panel may reasonably request in relation to the novation of the agreements referred to in Section M9.5 from the DCC to the Successor DCC.

M10. NOTICES

Communication via Specified Interfaces

M10.1 This Code requires certain communications to be sent via certain specified means, including as described in:

(a) Section E2 (Provision of Registration Data);

(b) Section H3 (DCC User Interface);

(c) Section H8 (Service Management, Self-Service Interface and Service Desk); and

(d) Section L4 (The SMKI Service Interface) and L5 (The SMKI Repository Interface).

Other Notices

M10.2 Save as referred to in Section M10.1, any notice or other communication to be made by one Party to another Party under or in connection with this Code or any Bilateral Agreement shall be in writing and shall be:

(a) delivered personally or by courier;

(b) sent by first class prepaid post; or

(c) sent by fax or email.

M10.3 All notices and communications as described in Section M10.2 shall be sent to the physical address, fax number or email address specified for such purpose in the relevant Party's Party Details. Where no fax or email address is specified for a particular type of notice or communication, notice may not be given in that manner.

M10.4 Subject to Section M10.5, all notices and communications as described in Section M10.2 shall be deemed to be received by the recipient:

(a) if delivered personally or by courier, when left at the address set out for such purpose in the relevant Party's Party Details;

(b) if sent by first class prepaid post, two Working Days after the date of posting;

(c) if sent by fax, upon production by the sender's equipment of a transmission report indicating that the fax was sent to the fax number of the recipient in full without error; and

(d) if sent by email, one hour after being sent, unless an error message is received by the sender in respect of that email before that hour has elapsed.

M10.5 Any notice that would otherwise be deemed to be received on a day that is not a Working Day, or after 17.30 hours on a Working Day, shall be deemed to have been received at 9.00 hours on the next following Working Day.

The Panel, Code Administrator, Secretariat and SECCo

M10.6 Notices between a Party and any of the Panel, the Code Administrator, the Secretariat or SECCo shall also be subject to this Section M. Notices to any of the Panel, the Code Administrator, the Secretariat or SECCo shall be sent to the relevant address given for such purpose, from time to time, on the Website (or, in the absence of any such address, to SECCo's registered office).

Process Agent

M10.7 Any Party (being a natural person) who is not resident in Great Britain or (not being a natural person) which is not incorporated in Great Britain shall, as part of its Party Details, provide an address in Great Britain for service of process on its behalf in any proceedings under or in relation to this Code and/or any Bilateral Agreement. Where any such Party fails at any time to provide such address, such Party shall be deemed to have appointed SECCo as its agent to accept such service of process on its behalf.

M11. MISCELLANEOUS

Entire Code

M11.1 This Code and any document referred to herein represents the entirety of the contractual arrangements between the Parties in relation to the subject matter of this Code. This Code and any document referred to herein supersedes any previous contract between any of the Parties with respect to the subject matter of this Code.

M11.2 Each Party confirms that, except as provided in this Code and without prejudice to any claim for fraudulent misrepresentation, it has not relied on any representation, warranty or undertaking which is not contained in this Code or any document referred to herein.

Severability

M11.3 If any provision of this Code shall be held to be invalid or unenforceable by a judgement or decision of any Competent Authority, that provision shall be deemed severable and the remainder of this Code shall remain valid and enforceable to the fullest extent permitted by law.

Waivers

M11.4 The failure by any Party to exercise, or the delay by any Party in exercising, any right, power, privilege or remedy provided under this Code or by law shall not constitute a waiver thereof nor of any other right, power, privilege or remedy. No single or partial exercise of any such right, power, privilege or remedy shall preclude any future exercise thereof or the exercise of any other right, power, privilege or remedy.

Third Party Rights

M11.5 The following persons shall be entitled to enforce the following rights in accordance with the Contracts (Rights of Third Parties) Act 1999:

(a) the person referred to in Sections C3.12 (Protections for Panel Members and Others) and M2.13(a) (Other Matters) shall be entitled to enforce the respective rights referred to in those Sections;

(b) the Approved Finance Party for each Communications Hub Finance Facility shall be entitled to exercise and/or enforce the following rights of the DCC in respect of the Communications Hub Finance Charges relating to that facility where a Communications Hub Finance Acceleration Event has occurred in respect of that Communications Hub Finance Facility and the Authority has determined that the DCC is unwilling or unable to do so:

(i) the right to calculate the amount of the Communications Hub Finance Charges arising as a result of that event (provided in such circumstances that the Approved Finance Party must demonstrate to the satisfaction of the Authority that the amount of the charges so calculated will in aggregate be no more than the amount contractually due and payable (but unpaid) by the DCC to the Approved Finance Party in respect of that event);

(ii) the right to invoice the Users in respect of the Communications Hub Finance Charges arising as a result of the Communications Hub Finance Acceleration Event (whether in the amount calculated by the DCC in accordance with this Code, or in the amount calculated by the Approved Finance Party and approved by the Authority under Section M11.5(b)); and/or

(iii) the right to enforce payment by the Users in accordance with this Code of the amount of Communications Hub Finance Charges invoiced in accordance with this Code,

and the payment of any amount by a User to an Approved Finance Party pursuant to this Section M11.5(b) shall satisfy that User's obligation to pay that amount to the DCC; and

(c) the Approved Finance Party for each 4G DBT Finance Facility shall be entitled to exercise and/or enforce the following rights of the DCC in respect of the 4G DBT Finance Charges relating to that facility where a 4G DBT Finance Acceleration Event has occurred in respect of that 4G DBT Finance Facility and the Authority has determined that the DCC is unwilling or unable to do so:

(i) the right to calculate the amount of the 4G DBT Finance Charges arising as a result of that event (provided in such circumstances that the Approved Finance Party must demonstrate to the satisfaction of the Authority that the amount of the charges so calculated will in aggregate be no more than the amount contractually due and payable (but unpaid) by the DCC to the Approved Finance Party in respect of that event);

(ii) the right to invoice the Users in respect of the 4G DBT Finance Charges arising as a result of the 4G DBT Finance Acceleration Event (whether in the amount calculated by the DCC in accordance with this Code, or in the amount calculated by the Approved Finance Party and approved by the Authority under Section M11.5(c)); and/or

(iii) the right to enforce payment by the Users in accordance with this Code of the amount of 4G DBT Finance Charges invoiced in accordance with this Code,

and the payment of any amount by a User to an Approved Finance Party pursuant to this Section M11.5(c) shall satisfy that User's obligation to pay that amount to the DCC; and

(d) AltHANCo (as defined in Section Z (Alt HAN Arrangements)) shall be entitled to enforce all rights which are conferred upon it under Section Z4 (Alt HAN Costs and Budgets), and shall (notwithstanding Section M11.8) be entitled to assign the benefit of these rights.

M11.6 Subject to Section M11.5, the Parties do not intend that any of the terms or conditions of this Code will be enforceable by a third party (whether by virtue of the Contracts (Rights of Third Parties) Act 1999 or otherwise).

M11.7 Notwithstanding that a person who is not a Party has the right to exercise and/or enforce particular rights in accordance with Section M11.5, the Parties may vary or terminate this Code in accordance with its terms without requiring the consent of any such person.

Assignment and Sub-contracting

M11.8 Without prejudice to a Party's right to appoint agents to exercise that Party's rights, no Party may assign any of its rights under this Code without the prior written consent of the other Parties.

M11.9 Any Party may sub-contract or delegate the performance of any or all of its obligations under this Code to any appropriately qualified and experienced third party, but such Party shall at all times remain liable for the performance of such obligations (and for the acts and omissions of such third party, as if they were the Party's own). It is expressly acknowledged that the DCC has sub-contracted a number of its obligations under this Code to the DCC Service Providers.

Agency

M11.10 Nothing in this Code shall create, or be deemed to create, a partnership or joint venture or relationship of employer and employee or principal and agent between the Parties and no employee of one Party shall be deemed to be or have become an employee of another Party.

M11.11 No Party shall:

(a) pledge the credit of another Party;

(b) represent itself as being another Party, or an agent, partner, employee or representative of another Party; or

(c) hold itself out as having any power or authority to incur any obligation of any nature, express or implied, on behalf of another Party.

Derogations

M11.12 A Party that holds an Energy Licence shall not be obliged to comply with its obligations under this Code to the extent to which such Party has the benefit of a derogation from the obligation to do so granted by the Authority under such Energy Licence.

Law and Jurisdiction

M11.13 This Code and any dispute or claim arising out of or in connection with it (including non-contractual claims) shall be governed by, and construed in accordance with, the laws of England and Wales.

M11.14 In relation to any dispute or claim arising out of or in connection with this Code (including in respect of non-contractual claims), each Party (subject to Section M7 (Dispute Resolution)) irrevocably agrees to submit to the exclusive jurisdiction of the courts of England and Wales and of Scotland. For the avoidance of doubt, the foregoing shall not limit a Party's right to enforce a judgment or order in any other jurisdiction.

SECCo

M11.15 The provisions of this Section M11 (and the definitions used in this Section) shall apply to SECCo as if SECCo was a Party.

N SMETS1 METERS

N1. DEFINITIONS FOR THIS SECTION N

N1.1 In this Section N, unless the context otherwise requires, the expressions in the left-hand column below shall have the meanings given to them in the right-hand column below:

Adoption means, in respect of a Communications Contract, to novate (with or without amendment) some or all of the Supplier Party's rights and obligations under the contract (to the extent arising after the date of novation) to the DCC; and "**Adopt**", "**Adopting**" and "**Adopted**" shall be interpreted accordingly.

Adoption Criteria means the non-exhaustive criteria (including those set out in Section N3.7) against which the DCC will analyse and report upon the feasibility and cost of Adopting a Communications Contract in order to facilitate the provision by the DCC of the Minimum SMETS1 Services in respect of the Eligible Meters that are the subject of that contract.

Communications Contract means, in respect of an Energy Meter, the contract or contracts (or the relevant parts thereof) pursuant to which the Supplier Party has (or, will following installation, have) the right to receive communication services in respect of that Energy Meter.

Eligible Meter means, in respect of each Supplier Party, an Energy Meter which is:
(a) either a SMETS1 Meter or subject to an upgrade plan which will result in it being a SMETS1 Meter prior to its Enrolment; and
(b) installed at premises (or planned to be installed at premises) for which that Supplier Party is an energy supplier.

Enrolment means, in respect of a SMETS1 Meter, the establishment by the DCC of communications with the SMETS1 Meter such that the DCC can (on an ongoing basis) provide the SMETS1 Services in respect of the SMETS1 Meter (and the words "**Enrol**" and "**Enrolled**" will be interpreted accordingly).

Initial Enrolment means the Enrolment of some or all of the Eligible Meters which were included within the scope of the Initial Enrolment Project Feasibility Report or within the scope of any additional analysis pursuant to Section N4A (Further Initial Enrolment Analysis).

Initial Enrolment Code Amendments has the meaning given to that expression in Section N3.1 (Overview of Initial Enrolment).

Initial Enrolment Project Feasibility Report has the meaning given to that expression in Section N3.1 (Overview of Initial Enrolment).

Minimum SMETS1 Services means those communication services described in Appendix F (Minimum Communication Services for SMETS1 Meters).

SMETS1 Meter means:

a. an Electricity Meter that has (as a minimum) the functional capability specified by and complies with the other requirements of a Version of the ESMETS with a Principal Version number of 1 (but not a Version of the ESMETS with a Principal Version number of greater than 1); or

b. a Gas Meter that has (as a minimum) the functional capability specified by and complies with the other requirements of a Version of the GSMETS with a Principal Version number of 1 (but not a Version of the GSMETS with a Principal Version number of greater than 1).

SMETS1 Services means those communication services described in Section N2.2 (SMETS1 Services).

N1.2 To the extent that Section A1.1 (Definitions) contains the same defined expressions as are set out in Section N1.1, the defined expressions in Section A1.1 shall not apply to this Section N.

N1.3 The expressions used in this Section N that are to have the meanings given in Section A1.1 (Definitions) and which have a meaning which relates directly or indirectly to the provision of Services in connection with Smart Metering Systems shall be interpreted by reference to the purposes of this Section N (including the purpose of establishing the feasibility, cost and means of providing the SMETS1 Services in connection with the SMETS1 Meters).

N2. SMETS1 ENROLMENT PROJECTS GENERALLY

Overview

N2.1 This Section N2 sets out certain matters which will apply to all projects to Enrol SMETS1 Meters, regardless of whether this is pursuant to the Initial Enrolment Code Amendments or any subsequent Modification Proposal.

SMETS1 Services

N2.2 The communication services to be provided in respect of particular SMETS1 Meters (the "**SMETS1 Services**") shall:

(a) be set out in the amendments to this Code (or where any such amendments have been proposed but not yet made, in such proposed amendments to this Code) pursuant to which those SMETS1 Meters become eligible for Enrolment; or

(b) prior to any such amendments being proposed, be determined in accordance with the Secretary of State's directions from time to time under Section N4A (Further Initial Enrolment Analysis).

N2.3 Not used

N2.4 Not used

N2.5 Not used

N2.6 Not used

N2.7 Not used

Testing

N2.8 Before Enrolling one or more SMETS1 Meters of a particular type, the DCC shall ensure that it has tested the DCC Systems and its processes to demonstrate that it is capable of discharging its obligations and exercising its rights under this Code (as amended pursuant to the Initial Enrolment Code Amendments or any subsequent Modification Proposal) in respect of that type of SMETS1 Meter.

N2.9 In discharging its obligations under Section N2.8, the DCC must prepare and follow an approach to testing that is (to the extent that it is appropriate to do so given the purpose for which the testing is being undertaken) consistent with the approach to testing set out in Section T (Testing During Transition). Where Section T has ceased to apply, this Section N2.9 shall be taken to refer to the provisions of Section T that applied immediately before it ceased to apply.

Security

N2.10 In producing the Initial Enrolment Project Feasibility Report or analysing and reporting on any subsequent Modification Proposal relating to the Enrolment of SMETS1 Meters, the DCC shall:

(a) prepare a risk assessment detailing the security risks associated with operating and using the SMETS1 Services;

(b) detail the measures (including Systems) proposed in order to ensure that the level of security risk to the DCC Total System, Enrolled Smart Metering Systems and/or User Systems will not be materially increased as a consequence of the provision of the SMETS1 Services; and

(c) prepare a risk treatment plan outlining the residual risks which exist once the measures referred to above have been taken.

N2.11 For the purposes of Section N2.10, the expressions Enrolled Smart Metering Systems, DCC Total System, and User Systems shall, when assessing the security risks that will apply as a consequence of the provision of the SMETS1 Services in respect of SMETS1 Meters, be interpreted so as to also include (respectively) those SMETS1 Meters and all additional Systems of the DCC and Users that would be used in relation to those SMETS1 Services.

In discharging its obligations under Section N2.10, the DCC shall consult with the Security Sub-Committee, and shall document the extent to which the views of the Security Sub-Committee have been taken into account.

N3. INITIAL ENROLMENT

Overview of Initial Enrolment

N3.1 This Section N3 together with Sections N4, N4A and N5 sets out the process by which the DCC will:

(a) analyse, evaluate and report (the “**Initial Enrolment Project Feasibility Report**”) to the Secretary of State regarding the feasibility and cost of the options for Initial Enrolment;

(b) undertake further analysis and evaluation as directed by the Secretary of State under Section N4A (Further Initial Enrolment Analysis); and

(c) prepare one or more sets of proposed amendments to this Code (the "**Initial Enrolment Code Amendments**") designed to deliver Initial Enrolment.

N3.2 The DCC shall comply with the Secretary of State’s directions from time to time regarding:

(a) the scope of the Initial Enrolment Project Feasibility Report;

(b) the scope and number of the Initial Enrolment Code Amendments to be prepared; and

(c) the timing and process to be followed by the DCC in relation to the production of the Initial Enrolment Project Feasibility Report and the Initial Enrolment Code Amendments.

DCC’s Invitation

N3.3 Where, and by such date as, the Secretary of State may direct for the purposes of this Section N3.3, the DCC shall send an invitation to each Supplier Party seeking details of the Energy Meters of that Supplier Party which the Supplier Party wishes to be included within the scope of the Initial Enrolment Project Feasibility Report.

N3.4 Each Supplier Party undertakes that it shall not propose Energy Meters to be included within the scope of the Initial Enrolment Project Feasibility Report unless those Energy Meters are Eligible Meters, and shall confirm to the DCC that the Energy Meters that it proposes are Eligible Meters. The DCC shall not be obliged to determine whether the Energy Meters proposed by each Supplier Party are Eligible Meters, and shall rely upon the confirmation provided by each Supplier Party.

N3.5 The DCC shall provide a copy of its invitation pursuant to Section N3.3 to the Secretary of State, the Authority and the Panel, and shall arrange for its publication on the DCC Website.

N3.6 The DCC’s invitation pursuant to Section N3.3 shall specify:

(a) the reasonable date by which Supplier Parties must respond in order for their Energy Meters to be included within the scope of the Initial Enrolment Project Feasibility Report;

(b) the reasonable format in which Supplier Parties must respond in order for their Energy Meters to be included within the scope of the Initial Enrolment Project Feasibility Report;

(c) any reasonable information which Supplier Parties must provide in order for their Energy Meters to be included within the scope of the Initial Enrolment Project Feasibility Report (which will include such details as the DCC shall specify regarding the Communications Contracts relating to those Energy Meters); and

(d) the Adoption Criteria.

N3.7 The Adoption Criteria specified by the DCC must include reference to Communications Contract provisions relating to the following concepts:

(a) novation;

(b) termination;

(c) liability;

(d) exclusivity and restrictions on competing activities;

(e) data ownership and security;

(f) confidentiality; and

(g) disaster recovery, business continuity and incident management.

N3.8 The DCC must respond in a timely manner to reasonable clarification requests from Supplier Parties regarding the DCC's invitation pursuant to Section N3.3, and any further information requests made by the DCC pursuant to this Section N3.

Suppliers' Response

N3.9 No Supplier Party is obliged to propose Energy Meters to be included within the scope of the Initial Enrolment Project Feasibility Report.

N3.10 Each Supplier Party that wishes to propose any or all of its Energy Meters for inclusion within the scope of the Initial Enrolment Project Feasibility Report must provide the DCC with the information in respect of those Energy Meters required by the DCC pursuant to this Section N3 by the date and in the format required by the DCC pursuant to this Section N3.

N3.11 Following receipt of each response from a Supplier Party pursuant to this Section N3, the DCC shall review the response to establish whether it complies with the requirements of this Section N3. Where a response is incomplete or the DCC reasonably requires supplementary information in respect of a response, the DCC may request that further information is provided within a reasonable period. The DCC must request further or supplementary information where it considers that the initial information provided by a Supplier Party is not sufficient to enable the DCC to include the Supplier Party's Energy Meters within the scope of the Initial Enrolment Project Feasibility Report.

Inclusion of Meters in Scope of Project

N3.12 The Energy Meters of a Supplier Party shall only be included within the scope of the Initial Enrolment Project Feasibility Report where the Supplier Party has provided all of the information in respect of those Energy Meters required by the DCC pursuant to this Section N3 by the date and in the format required by the DCC in accordance with this Section N3.

N3.13 In respect of each Energy Meter put forward by a Supplier Party, the DCC shall notify that Supplier Party whether the DCC considers that Energy Meter to be within (or outside) the scope of the Initial Enrolment Project Feasibility Report (determined as described in Section N3.12).

Disputes

N3.14 Without prejudice to Section N2.7 (SMETS1 Compliance), where:

(a) the DCC requests information from a Supplier Party pursuant to this Section N3, and the Supplier Party disputes whether that information has been requested in accordance with this Section N3; or

(b) a Supplier Party disagrees with the DCC's notification that some or all of the Supplier Party’s Energy Meters are outside the scope of the Initial Enrolment Project Feasibility Report,

then the Supplier Party may refer the matter to the Secretary of State (whose decision shall be final and binding for the purposes of this Code).

N4. INITIAL ENROLMENT PROJECT FEASIBILITY REPORT

Analysis

N4.1 The DCC shall analyse the information received from Supplier Parties pursuant to Section N3, evaluate the options for Initial Enrolment that the DCC considers are reasonable, and report to the Secretary of State in the Initial Enrolment Project Feasibility Report on the feasibility and estimated cost of each option and the manner in which it would be delivered.

Timetable

N4.2 As soon as reasonably practicable following receipt of the relevant information from Supplier Parties pursuant to Section N3, the DCC shall publish on the DCC Website its proposed timetable for undertaking the steps required under this Section N4.

Report

N4.3 The DCC shall include within the Initial Enrolment Project Feasibility Report the DCC’s analysis regarding the options for the Enrolment of all the Eligible Meters which were included within the scope of the Initial Enrolment Project Feasibility Report. Where the Enrolment of one or more subsets of such Eligible Meters would differ materially from the Enrolment of all of such Eligible Meters (in terms of risk, timescales and/or cost), then the DCC shall include its analysis for that subset (as well as for all of them).

N4.4 The DCC shall include within the Initial Enrolment Project Feasibility Report the DCC’s analysis regarding the following matters in respect of the Enrolment of all (and, where applicable in accordance with Section N4.3, each subset referred to in that Section) of the Eligible Meters which were included within the scope of the Initial Enrolment Project Feasibility Report:

(a) the timeframe and process for the Enrolment of the Eligible Meters;

(b) its assessment of the Communications Contracts against the Adoption Criteria, and of whether some or all of the Communications Contracts should be Adopted, and of whether those that are to be Adopted should be amended or consolidated following their Adoption;

(c) any amendments that would be required to existing DCC Service Provider Contracts in order to deliver Initial Enrolment;

(d) the establishment of any new contracts which the DCC would require in order to deliver Initial Enrolment;

(e) the means by which the DCC will provide SMETS1 Services in respect of the Eligible Meters such that (insofar as reasonably practicable) Users may send Service Requests and receive Service

Responses in respect of those communication services via the DCC User Interface (such that the format of communications over the DCC User Interface in relation to each SMETS1 Service is the same as that for existing equivalent DCC User Interface Services);

(f) where it better facilitates achievement of the SEC Objectives, the provision by the DCC to Users of the SMETS1 Services in respect of the Eligible Meters by another means than that referred to in (e) above;

(g) to the extent that they can be offered without a material increase in cost, risk or timescale, any rights for Parties also to Enrol SMETS1 Meters which were not included within the scope of the Initial Enrolment Project Feasibility Report;

(h) options for amendment of the Minimum SMETS1 Services such that DCC can provide additional Services to Parties which are equivalent to the DCC User Interface Services;

(i) options for provision by DCC to Users of a service for Eligible Meters to be commissioned first in the DCC (in addition to Enrolment post-commissioning);

(j) any Enabling Services that the DCC considers necessary to support Enrolment (including the equivalent of Testing Services);

(k) the development and testing of the Systems via which the Enrolment of Eligible Meters and provision of SMETS1 Services will be delivered, in compliance with the requirements of Section N2.8 (Testing);

(l) the measures proposed in order to ensure that the SMETS1 Services are delivered in a manner that will not materially increase the security risk, in compliance with the requirements of Section N2.10 (Security);

(m) an assessment of which Supplier Parties are (in accordance with the Charging Objectives) likely to pay a premium and its reasonable estimate of the amount of those premiums in respect of Enrolled SMETS1 Meters (over and above the Charges for Smart Metering Systems); and

(n) other matters required to be considered in compliance with the requirements of Section N2 (SMETS1 Enrolment Projects Generally).

Consultation

N4.5 Before submitting the Initial Enrolment Project Feasibility Report to the Secretary of State, the DCC shall produce a draft report and consult with the Panel, the Parties and other interested persons concerning the content of such draft. The DCC shall ensure that a reasonable period of time is allowed for consultation responses to be made, which period may not be less than two months.

N4.6 On submitting the Initial Enrolment Project Feasibility Report to the Secretary of State, the DCC shall also provide the Secretary of State with:

(a) copies of all consultation responses received;

(b) a commentary identifying where and the extent to which the DCC has amended its report to take into account any comments, representations or objections raised as part of such consultation responses; and

(c) where the DCC has not amended the report to address any comments or representations of objections raised as part of such consultation responses, the DCC's reasons for not doing so.

Inclusion or Exclusion of Meters from Scope of Report

N4.7 Before submitting the Initial Enrolment Project Feasibility Report to the Secretary of State, the DCC shall (subject to Section N4.11) publish a final draft of the report in the form it intends to submit to the Secretary of State (subject only to Section N4.9).

N4.8 On publishing the draft report pursuant to Section N4.7, the DCC shall notify the Supplier Parties that they each have two weeks to notify the DCC if they wish to include additional Energy Meters, or exclude some or all of their Energy Meters, from some or all of the options within the scope of the Initial Enrolment Project Feasibility Report. If no response is received from a Supplier Party within that period, the DCC shall assume that all of the Energy Meters previously included within the scope of the report remain within scope.

N4.9 The DCC shall include or exclude (as applicable) from the scope of the Initial Enrolment Project Feasibility Report those Energy Meters notified in accordance with Section N4.8, and:

(a) where the DCC considers that the inclusion or exclusion of those Energy Meters has a material impact on the Initial Enrolment Project Feasibility Report, then the DCC shall produce a further draft of the report, and undertake a further consultation in accordance with Section N4.5 (but without repeating the steps at Section N4.7 and N4.8); or

(b) where the DCC considers that the inclusion or exclusion of those Energy Meters does not have a material impact on the Initial Enrolment Project Feasibility Report, then the DCC shall amend the report only insofar as necessary to include or exclude those Energy Meters from the scope of the report and submit the report to the Secretary of State.

Redaction for Reasons of Security

N4.10 Before consulting on or publishing the draft report pursuant to Section N4.5 or N4.7, the DCC shall provide to the Panel and (on request) the Secretary of State:

(a) a copy of the draft report; and

(b) where relevant, a list of sections of the report which the DCC considers should be redacted prior to publication in order to avoid a risk of Compromise to the DCC Total System and/or User Systems .

N4.11 The DCC shall only consult on or publish its draft report pursuant to Section N4.5 or N4.7 after it has redacted those sections of the report which it is directed to redact by the Panel where the Panel considers that those sections contain information which may pose a risk of Compromise to the DCC Total System and/or User Systems (which sections may or may not include those sections which the DCC proposed for redaction).

N4A FURTHER INITIAL ENROLMENT ANALYSIS

Further Analysis and Reporting

N4A.1 Where from time to time directed to do so by the Secretary of State, the DCC shall undertake further analysis and/or evaluation relating to Initial Enrolment, and report to the Secretary of State on such analysis and/or evaluation.

N4A.2 The DCC shall comply with the Secretary of State's directions from time to time pursuant to this Section N4A, which may include directions in relation to one or more of the following:

(a) additional Energy Meters which are to be included within the scope of Initial Enrolment (including in terms of either or both Device Models or numbers of Energy Meters);

(b) Energy Meters which are to be excluded from the scope of Initial Enrolment (including in terms of either or both Device Models or numbers of Energy Meters);

(c) the aspects of Initial Enrolment that are to be further analysed and/or evaluated;

(d) consultation with such persons as the Secretary of State may direct regarding Initial Enrolment and/or the DCC's analysis and/or evaluation;

(e) further invitations to Supplier Parties to have additional Energy Meters included within the scope of Initial Enrolment;

(f) the timing and process to be followed by the DCC in relation to the further analysis and/or evaluation, and/or any consultation or information requests relating to such analysis and/or evaluation; and

(g) redaction of published information equivalent to that outlined in Section N4.10 (Redaction for Reasons of Security).

Supplier Information

N4A.3 The DCC may request information from Supplier Parties in relation to any further analysis and/or evaluation which the DCC is required to undertake under this Section N4A, where:

(a) such information is reasonably necessary for the purpose of the analysis and/or evaluation which the DCC is required to undertake (which may include copies of Communications Contracts); or

(b) the DCC is directed by the Secretary of State to request such information.

N4A.4 Each information request pursuant to Section N4A.3 must specify a reasonable date and a reasonable format for responses by Supplier Parties.

N4A.5 Each Supplier Party which wants its Energy Meters to remain within the scope of Initial Enrolment shall take all reasonable steps to provide the information requested by the DCC in accordance with Section N4A.3.

N4A.6 Where a Supplier Party does not provide the information requested by the DCC under Section N4A.3, and where the DCC considers that its analysis and/or evaluation cannot be completed in relation to that Supplier Party's Energy Meters without such information, then the DCC may apply to the Secretary of State to determine whether all (or a subset) of that Supplier Party's Energy Meters should be excluded from the scope of Initial Enrolment.

N4A.7 In respect of each response from a Supplier Party to a DCC request pursuant to Section N4A.3, the DCC shall notify the Supplier Party whether the DCC considers that the response has been made in accordance with the request (identifying any omissions or other deficiencies and allowing a reasonable period of time within which such omissions or other deficiencies can be rectified).

N4A.8 For the avoidance of doubt, the DCC shall only use the information obtained pursuant to this Section N4A for the purposes of the further analysis and/or evaluation required by this Section N4A, and all information obtained pursuant to this Section N4A shall be subject to the DCC's duties of confidentiality set out in the DCC Licence and Section M4 (Confidentiality).

N5. INITIAL ENROLMENT CODE AMENDMENTS

Amendments

N5.1 Where directed to do so by the Secretary of State, the DCC shall prepare Initial Enrolment Code Amendments in respect of one or more options for Initial Enrolment in respect of some or all of the Eligible Meters included within the scope of the Initial Enrolment Project Feasibility Report or included within the scope of any further analysis and/or evaluation pursuant to Section N4A (as directed by the Secretary of State).

N5.2 Such amendments shall include those necessary to enable the Enrolment of the relevant SMETS1 Meters, the request and receipt of SMETS1 Services in respect of those SMETS1 Meters, and the calculation of the Charges for the same in accordance with the Charging Objectives.

N5.3 Such amendments shall be prepared in a format capable of being laid before Parliament by the Secretary of State pursuant to section 88 of the Energy Act 2008.

Consultation

N5.4 Before submitting the Initial Enrolment Code Amendments to the Secretary of State pursuant to Section N5.1, the DCC shall produce draft amendments and consult with the Authority, the Panel, the Parties and other interested persons concerning such draft. The DCC shall ensure that a reasonable period of time is allowed for consultation responses to be made, which period may not be less than two months.

N5.5 On submitting the Initial Enrolment Code Amendments to the Secretary of State, the DCC shall also provide the Secretary of State with:

(a) copies of all consultation responses received;

(b) a commentary identifying where and the extent to which the DCC has amended its draft to take into account any comments, representations or objections raised as part of such consultation responses; and

(c) where the DCC has not amended its draft to address any comments or representations of objections raised as part of such consultation responses, the DCC’s reasons for not doing so.

N6. TRANSITION AND MIGRATION APPROACH DOCUMENT

Overview

N6.1 The Transition and Migration Approach Document is to be developed by the DCC pursuant to this Section N6, and incorporated into this Code pursuant to Part G of Condition 22 of the DCC Licence and Section X5 (Incorporation of Certain Documents into this Code).

Purpose of the Transition and Migration Approach Document

N6.2 The purposes of the Transition and Migration Approach Document are to:

(a) enable the Enrolment of SMETS1 Smart Metering Systems comprising SMETS 1 Devices that have previously been commissioned by a SMETS1 SMSO (whether or not they remain so commissioned immediately prior to their Enrolment);

(b) provide for additional and/or varied provisions to apply for a transitional period prior to, during and/or following the Enrolment of such SMETS1 Smart Metering Systems.; and

(c) facilitate the provision of Elective Communication Services in respect of SMETS 1 Smart Metering Systems.

Content of the Transition and Migration Approach Document

N6.3 The Transition and Migration Approach Document may include, without limitation, some or all of the following:

(a) rights and/or obligations of the DCC and other Parties designed to facilitate or achieve the purposes of the Transition and Migration Approach Document which are either additional to or vary other rights and/or obligations set out in this Code;

(b) the processes by which SMETS 1 Devices that have previously been commissioned by a SMETS1 SMSO may be Commissioned and Enrolled as SMETS1 Smart Metering Systems (which may include obligations to apply before, on and/or after such Commissioning);

(c) pre-conditions to apply in relation to the Commissioning of SMETS1 Devices, including by reference to the DCC, SMETS1 Device Model, Lead Supplier, Responsible Supplier, the SMETS1 SMSO by which the SMETS1 Devices were previously commissioned, and/or the Supplier Party by which the SMETS1 Devices were originally installed;

(d) rules and constraints concerning the scheduling and timing to be followed in respect of the Commissioning of SMETS1 Devices, including by reference to the relevant SMETS1 Device Model, Lead Supplier, Responsible Supplier, SMETS1 Service Provider, SMETS1 SMSO by which the SMETS1 Devices were previously commissioned, and/or Supplier Party by which the SMETS1 Devices were originally installed;

(e) obligations on one or more Parties to procure that SMETS1 SMSOs undertake specified activities to support the Enrolment of SMETS1 Smart Metering Systems;

(f) rules and requirements concerning the provision and sharing of Data in order to facilitate or achieve the purposes of the Transition and Migration Approach Document, which may include one or more

Parties being obliged to provide (or procure the provision of) Data (as further described in the Transition and Migration Approach Document);

(g) provisions concerning the re-configuration of SMETS1 Devices and/or the taking over and handing back of communications with SMETS1 Devices, which may include one or more Parties being obliged to make arrangements for the same (as further described in the Transition and Migration Approach Document);

(h) provisions concerning the exchange of security keys, security credentials and/or cryptographic material, which may include modification of the SMKI Services and the SMKI Repository Service to permit the Issuing of Organisation Certificates with additional Remote Party Roles (and their lodging in the SMKI Repository);

(i) provisions requiring the DCC and Users to enter into Bilateral Agreements for the provision of certain Elective Communication Services in respect of SMETS 1 Smart Metering Systems;

(j) provisions that permit the population and/or amendment of the Central Products List, SMETS1 Eligible Product Combinations, SMETS1Pending Product Combinations and/or the Smart Metering Inventory other than by means of the enduring arrangements;

(k) limitations and/or variations to the Services and/or the rights and/or obligations of the Parties to apply for a transitional period prior to and/or following the Enrolment of some or all SMETS1 Smart Metering Systems, which may include limitations and/or variations to Services in respect of SMETS2 Devices;

(l) the variation of limitations on liability provided for in this Code for a transitional period prior to and/or following the Enrolment of some or all SMETS1 Smart Metering Systems, and provision for the giving of indemnities against liabilities to which one or more Parties and/or SMETS1 SMSOs might be exposed in consequence of the Transition and Migration Approach Document;

(m) provision for SMETS1 SMSOs to be given rights to enforce certain provisions of the Transition and Migration Approach Document in accordance with the Contracts (Rights of Third Parties) Act 1999, notwithstanding Section M11.5 (Third Party Rights); and

(n) provision for the referral and determination of disputes in respect of the Transition and Migration Approach Document, which may include interim or final determinations by the Secretary of State, the Authority, the Panel or any other person specified by the Secretary of State.

Process to Develop Document for Designation

N6.4 The DCC shall, to the extent it has not already done so when this Section N6 comes into effect, develop and consult on the Transition and Migration Approach Document and submit it to the Secretary of State in accordance with the following process:

(a) the DCC shall, in consultation with the Parties and such other persons as are likely to be interested, produce a draft of the document;

(b) where a disagreement arises with any Party or other person with regard to any proposal as to the content of the document, the DCC shall endeavour to reach an agreed proposal with that person consistent with the purposes of the Transition and Migration Approach Document;

(c) the DCC shall send a draft of the Transition and Migration Approach Document to the Secretary of State as soon as is practicable after completion of the process described in (a) and (b) above, and shall when doing so provide to the Secretary of State:

(i) a statement of the reasons why the DCC considers that draft to be fit for purpose;

(ii) copies of the consultation responses received; and

(iii) a summary of any disagreements that arose during consultation and that have not been resolved by reaching an agreed proposal; and

(d) the DCC shall comply with any requirements in a direction given to it by the Secretary of State in relation to the draft document, including:

(i) any amendments to be made to the draft document;

(ii) any requirement to produce and submit to the Secretary of State a further draft of the document; and

(iii) any requirement as to the process to be followed by the DCC (and the time within which that process shall be completed) prior to submitting a further such draft.

N6.5 The DCC shall, where so directed by the Secretary of State from time to time, develop and consult upon a further draft of the Transition and Migration Approach Document and submit it to the Secretary of State in accordance with the process set out in Section N6.4.

Application of the Transition and Migration Approach Document

N6.6 The DCC and the categories of Party referred to in the Transition and Migration Approach Document shall comply with the Transition and Migration Approach Document.

N6.7 The Transition and Migration Approach Document shall have priority over the other SEC Subsidiary Documents in relation to the subject matter of the Transition and Migration Approach Document.

Expiry of Transition and Migration Approach Document

N6.8 The Transition and Migration Approach Document shall provide for a date (or a mechanism for determining a date) from which the Transition and Migration Approach Document is to no longer apply. From such date, the Transition and Migration Approach Document shall no longer have any effect (but without prejudice to the rights and obligations arising prior to that date).

Interpretation

N6.9 Expressions used in this Section N6 and in the Transition and Migration Approach Document shall be interpreted in accordance with Section A (Definitions and Interpretation), rather than Section N1 (Definitions for this Section N).

P PRODUCTION PROVING

P1. PRODUCTION PROVING

Purpose

P1.1 The purpose of Production Proving is to provide assurance on the operation of the DCC Total System.

Overview

P1.2 The DCC may, in its capacity as the Production Proving Function and subject to this Section P, to the extent reasonably necessary for the purposes of Production Proving:

(a) act as if it is a User (in different User Roles) to send Service Requests;

(b) act as if it is a User (in different User Roles) to receive Service Responses and Alerts in relation to Production Proving Devices (as if it was an Eligible User);

(c) act as if it is a User (in different User Roles) to access the Self-Service Interface; and

(d) act as if it is the CSS Provider in respect of Production Proving Registration Data.

Production Proving Devices

P1.3 The Production Proving Function is only entitled to send a Service Request or Signed Pre-Command to the DCC that will result in communication with a Device where that Device is a Production Proving Device.

P1.4 A "**Production Proving Device**" is a (real) Device of a Device Model identified in the Central Products List, but one that has been procured by the DCC for the purposes of Production Proving.

P1.5 The Production Proving Function may send a Service Request requesting that the DCC adds a Production Proving Device to the Smart Metering Inventory (to be listed with an SMI Status of 'pending'), and the DCC shall add the Production Proving Device to the Smart Metering Inventory provided that the Production Proving Device is of a Device Model that is identified in the Central Products List.

P1.6 The Production Proving Function may install and Commission Production Proving Devices in order to create Smart Metering Systems, but those Production Proving Devices (and Smart Metering Systems) cannot be ones that record the supply of gas, or import or export of electricity, to or from a Premises for the purposes of settlement under the Energy Codes.

P1.7 The DCC shall not allow Production Proving Devices to be linked in the Smart Metering Inventory to (real) MPANs or MPRNs.

Production Proving MPXNs

P1.8 Given the limitation set out in Section P1.7, the Production Proving Function is entitled to generate dummy MPANs and dummy MPRNs (collectively, "**Production Proving MPXNs**") for the purposes of Production Proving. The DCC may record these Production Proving MPXNs in the Smart Metering Inventory and link them to Production Proving Devices for the purposes of recording the

Commissioning of Production Proving Devices. The DCC shall publish on the DCC Website the range of values which the DCC uses for Production Proving MPXNs.

P1.9 The Production Proving Function shall ensure that the Production Proving MPXNs are different from any and all MPANs and MPRNs, including that the data values of each Production Proving MPXN are outside the range that may in the future be used in an MPAN or MPRN.

P1.10 The DCC shall ensure that each Production Proving MPXN is only linked in the Smart Metering Inventory to a Production Proving Device (and not any other Device).

Production Proving Registration Data

P1.11 The Production Proving Function may generate dummy Registration Data ("**Production Proving Registration Data**") for the purposes of Production Proving.

P1.12 The Production Proving Function shall ensure that the data fields in the Production Proving Registration Data by which Parties and other market participants are identified all contain data values which are different from the values used in the Registration Data to identify Parties and other market participants, including that the data values are outside the range that may in the future be used to identify Parties and other market participants.

P1.13 The Production Proving Function shall be entitled to send the Production Proving Registration Data to the DCC in accordance with Section E (Registration Data) acting as if the Production Proving Function was the CSS Provider.

Excluded Service Requests

P1.14 The Production Proving Function may not submit the following Service Requests (or send Signed Pre-Commands that relate to the following Service Requests):

(a) Update Security Credentials (KRP) (SRV 6.15);

(b) Request Handover Of DCC Controlled Device (SRV 6.21); or

(c) Update Security Credentials (CoS) (SRV 6.23).

Testing

P1.15 The DCC shall, before it undertakes any or all of the activities set out in Section P1.2, successfully complete reasonable and appropriate testing of the Systems to be used as the Production Proving System.

P1.16 Prior to sending a Service Request to the DCC, the Production Proving Function must have successfully completed testing equivalent to User Entry Process Tests in the relevant User Role in which it wishes to act in sending that Service Request.

P1.17 Not used.

General Standards

P1.18 Where the DCC undertakes Production Proving, it shall do so in accordance with Good Industry Practice, and in a manner that does not adversely affect the provision of the Services.

Production Proving IDs

P1.19 The Panel shall, where requested by the DCC, issue one or more Party Signifiers to the DCC for the purposes of identifying the DCC when acting as if it was a User or a CSS Provider in its capacity as the Production Proving Function, and the Production Proving Function shall use these signifiers for such purpose.

P1.20 The Panel shall, where requested by the DCC, issue a new range of EUI-64 Compliant identifiers for use as DCC IDs by the DCC when acting as the Production Proving Function. This range must be outside the range of identifiers used by DCC as DCC IDs for any other DCC purpose under this Code.

P1.21 The DCC shall assign one or more DCC IDs for use only by the Production Proving Function.

P1.22 The DCC shall notify the Panel which DCC IDs are associated with which Production Proving Function Party Signifier.

P1.23 The Production Proving Function shall not use User IDs for the purpose of Production Proving.

Security

P1.24 As the Production Proving Systems form part of the DCC Live Systems and the DCC Total System, the DCC shall ensure that it complies with the relevant requirements of Section G (Security) which apply as a consequence.

P1.25 The Production Proving Systems do not need to comply with the requirements of Section G (Security) which apply to User Systems or which apply to the CSS Provider Systems (via Section E (Registration Data)); save that Section G6 (Anomaly Detection Thresholds: Obligations on the DCC and Users) shall apply to the Production Proving Function as if it was a User.

P1.26 For such purposes of Section G6 (Anomaly Detection Thresholds: Obligations on the DCC and Users), the Production Proving Function shall set Anomaly Detection Thresholds that have been approved by the Security Sub-Committee (and the DCC shall not process any communication from the Production Proving Function until such threshold values have been approved and set).

P1.27 In respect of the DCC's obligations under Section G6 (Anomaly Detection Thresholds: Obligations on the DCC and Users), not acting in the capacity of the Production Proving Function, the DCC shall set the Anomaly Detection Thresholds for the following Service Requests from the Production Proving Function to zero:

(a) Update Security Credentials (KRP) (SRV 6.15);

(b) Request Handover Of DCC Controlled Device (SRV 6.21); and

(c) Update Security Credentials (CoS) (SRV 6.23).

Records and Reporting to the Security Sub-Committee

P1.28 The DCC shall:

(a) retain an audit log of the activities undertaken by the Production Proving Function for at least 6 years from the date on which the activity was undertaken;

(b) carry out post-event checks to confirm that no Service Requests or Signed Pre- Commands sent by the Production Proving Function resulted in communication with a Device which is not a Production Proving Device (or would have resulted in such communication had the DCC not rejected the message); and

(c) carry out post-event checks to ensure that the Production Proving Registration Data did not contain any (real) MPANs or MPRNs and did not use identifiers that are (or have been) used in the Registration Data to identify Parties and other market participants.

P1.29 The DCC shall, within 5 Working Days following the end of each month, provide a report to the Security Sub-Committee which summarises in respect of that month the matters referred to in Section P1.28.

SMKI Services and DCCKI Services

P1.30 The Production Proving Function shall be entitled to receive SMKI Services and DCCKI Services under and in accordance with the relevant provisions of Section L (Smart Metering Key Infrastructure and DCC Key Infrastructure) and the SEC Subsidiary Documents applying pursuant to Section L as if it was a Party other than the DCC.

P1.31 The effect of Section P1.30 is to entitle the Production Proving Function to become an Authorised Subscriber, and to be an Eligible Subscriber in respect of those Device Certificates and Organisation Certificates for which the Production Proving Function is expressly stated to be eligible in Section L (Smart Metering Key Infrastructure and DCC Key Infrastructure).

P1.32 Before the Production Proving Function can apply to become an Authorised Subscriber or access the SMKI Repository, the Production Proving Function must have successfully completed testing equivalent to the SMKI and Repository Entry Process Tests.

P1.33 The Production Proving Function shall not submit any Certificate Signing Requests for a Device Certificate other than in relation to a Production Proving Device.

P1.34 The Production Proving Function shall not submit any Certificate Signing Request for an Organisation Certificate other than the one in relation to which it is identified as an Eligible Subscriber in Section L3 (The SMKI Services).

P1.35 The DCC is not required to implement controls within the DCA, an Issuing DCA or within the Registration Authority that limit the issuing of Device Certificates to the Production Proving Function in relation Production Proving Devices.

P1.36 The DCC shall ensure that no Public Key that is used by a Production Proving Device in relation to the Remote Party Role of either supplier or networkOperator is contained within any Certificate or other public key infrastructure certificate.

T TESTING DURING TRANSITION

[Not in use]

X TRANSITION

X1. GENERAL PROVISIONS REGARDING TRANSITION

Overriding Nature of this Section

X1.1 The provisions of this Section X shall apply notwithstanding, and shall override, any other provision of this Code.

Transition Objective

X1.2 The objective to be achieved pursuant to this Section X (the "**Transition Objective**") is the efficient, economical, co-ordinated, timely, and secure process of transition to the Completion of Implementation.

X1.3 The "**Completion of Implementation**" shall occur on the date designated for the purpose of this Section X1.3 by the Secretary of State (or such person as the Secretary of State may designate for the purposes of this Section X1.3), once the Secretary of State (or the person so designated) is of the opinion that:

(a) the documents referred to in Section X5 and that the Secretary of State (or the person so designated) considers material to the implementation of this Code have been incorporated into this Code in accordance with that Section;

(b) the provisions of this Code that the Secretary of State (or the person so designated) considers material to the implementation of this Code apply in full without any variation pursuant to this Section X (or, where any such variations do apply, the requirements of Sections X1.3(c) will still be met despite such variations ending in accordance with Section X1.5(a) and/or X1.5A(a)); and

(c) each Party that holds an Energy Licence is (or would be had such Party acted in accordance with Good Industry Practice) reasonably able (on the assumption that such Party acts in accordance with Good Industry Practice) to perform its obligations, and to exercise its rights, under this Code to the extent that the Secretary of State (or the person so designated) considers such obligations or rights material to the implementation of this Code.

X1.4 Before designating a date for the purpose of Section X1.3, the Secretary of State (or the person designated for the purposes of this Section X1.3) must consult the Authority, the Panel and the Parties in respect of the proposed date. Such consultation must allow such period of time as the Secretary of State (or the person so designated) considers appropriate in the circumstances within which representations or objections may be made.

Ending of the Application of this Section X

X1.5 With effect from the earlier of:

(a) Completion of Implementation; or

(b) 31 October 2018,

this Code shall automatically be modified so as to delete the following provisions of this Section X (and all variations to this Code provided for in, or made by directions pursuant to, the following provisions shall cease to apply):

(i) Section X1.11;

(ii) Section X2 (Effective Provisions at Designation), except for:

(A) Section X2.3(d), which shall continue to apply, but re-numbered as Section X2.1; and

(B) Sections X2.7 and X2.8, which shall continue to apply, but re- numbered as Sections X2.2 and X2.3 respectively;

(iii) Section X3 (Provisions to Become Effective Following Designation), except for:

(A) Section X3.1, which shall continue to apply, but amended to read: "Each Section, Schedule and SEC Subsidiary Document (or any part thereof) shall be effective, unless (at the time of a provision being added or modified by the Secretary of State pursuant to section 88 of the Energy Act 2008) the Secretary of State directs that such addition or modification is not to have effect, or is not to have effect until a later date. Where the Secretary of State directs that an addition or modification is not to have effect, the Secretary of State may subsequently designate a date from which it is to have effect."; and

(B) Section X3.9, which shall continue to apply, but re-numbered as X3.2;

(iv) Section X4 (Governance Set-up Arrangements);

(v) Section X6 (Transitional Variations);

(vi) Section X7 (Transitional Incident Management Procedures);

(vii) Section X8 (Developing CH Support Materials); and

(viii) Section X10 (Threshold Anomaly Detection Procedures).

X1.5A With effect from:

(a) Completion of Implementation:

(i) this Code shall automatically be modified so as to delete the provisions of this Section X not deleted pursuant to Section X1.5, save for Section X1.1, X1.3, this Section X1.5A, Section X5 and Section X11 which shall not be deleted; and

(ii) any variations to this Code provided for in, or made by directions pursuant to, the provisions deleted by Section X1.5A(a) shall cease to apply (save as set out in Section X5.8);

(b) 1 November 2028, this Section X (and any variations to this Code provided for in, or made by directions pursuant to, this Section X) shall cease to apply (save as set out in Section X5.8), and this Code shall automatically be modified from that date so as to delete this Section X.

General Obligations

X1.6 Each Party shall take all reasonable steps to do all such things as are within its power and necessary or expedient in order to facilitate achievement of the Transition Objective.

X1.7 Each Party shall provide such reasonable co-operation and assistance to the other Parties and to the Panel as may be necessary to facilitate compliance with the provisions of this Section X, and with any variations to this Code provided for in (or made by directions pursuant to) this Section X.

X1.8 Without prejudice to its legal rights, no Party shall take any step, or exercise any right, which is intended to (or might reasonably be expected to) hinder or frustrate the achievement of the Transition Objective.

Information

X1.9 Each Party shall provide to the Secretary of State, in such manner and at such times as the Secretary of State may reasonably require, such Data as the Secretary of State may reasonably require in order to enable the Secretary of State to assess progress towards (and to facilitate) achievement of the Transition Objective. No Party shall be obliged to provide information under this Section X1.9 where such Party is obliged to provide such information under its Energy Licence, or where such information is expressly excluded from the information that such Party is obliged to provide under its Energy Licence.

X1.10 If a Party is aware of any matter or circumstance which it considers will materially delay or frustrate the achievement of the Transition Objective, that Party shall promptly inform the Secretary of State of such matter or circumstance.

Network Parties to become Subscribers

X1.11 [NOT IN USE]

Day-One Elective Communication Services

X1.12 Where the Secretary of State designates one or more draft Bilateral Agreements for the purposes of this Section X1.12 (each of which drafts must specify the potential Elective Communication Services to be provided thereunder, and the DCC's potential counterparty thereunder), then:

(a) the DCC shall, within 10 Working Days thereafter, make a formal offer to each of the counterparties in question for the Elective Communication Services in question as if Section H7.12 (Formal Offer) applied;

(b) such offer shall be on the basis of the draft Bilateral Agreement designated by the Secretary of State (subject only to the addition of the applicable Elective Charges, any termination fee and any credit support requirements);

(c) the counterparty shall be under no obligation to accept such offer; and

(d) any agreement entered into pursuant to this Section X1.12 shall be a Bilateral Agreement.

Disputes

X1.13 In the event of any dispute between the Parties (or between the Panel and any Party) as to whether a particular Party is obliged to undertake a particular activity pursuant to Section X1.6 to X1.12 (inclusive), a Party (or the Panel) may refer the matter to the Secretary of State (or, where designated by the

Secretary of State for such purposes, the Panel or the Authority) for determination (which determination may include a requirement to comply with such terms and conditions as the person making it considers appropriate in all the circumstances of the case). Any determination by the Secretary of State or by the Authority pursuant to this Section X1.13 shall be final and binding for the purposes of this Section X1. Any determination by the Panel pursuant to this Section X1.13 shall be subject to appeal to the Secretary of State (or, where designated by the Secretary of State for such purposes, to the Authority), the determination of such appeal being final and binding for the purposes of this Section X1.

Modification of this Section X

X1.14 The variations to this Code provided for in, or made by directions pursuant to, this Section X shall not constitute modifications that should be subject to Section D (Modification Process). For the avoidance of doubt, this Section X shall be capable of being modified under Section D (Modification Process).

SECCo

X1.15 The provisions of this Section X1 (and the definitions used in this Section) shall apply to SECCo as if SECCo was a Party.

Publication of Draft Subsidiary Documents by the DCC

X1.16 Where, pursuant to this Code or the DCC Licence, the DCC is required to prepare or produce and to consult upon a draft (or further draft) of a document (or to resubmit a document) that is intended to be incorporated into this Code as a SEC Subsidiary Document, the DCC shall, at or around the same time as the DCC sends such document to the Secretary of State, publish on the DCC Website:

(a) a copy of the document sent to the Secretary of State; and

(b) a summary of any material comments raised in response to the consultation and a brief description of the reasons why any associated changes to the document were or were not made.

Testing in respect of Additional Release Services

X1.17 A Party seeking to become a User for a particular User Role must undertake the User Entry Process Tests relevant to that User Role, as described in Sections H1 (User Entry Process) and H14 (Testing). Certain Services are only available to Parties that have become a User for the applicable User Role, as described in Section H3 (DCC User Interface) and the DCC User Interface Services Schedule. Where the Secretary of State makes directions pursuant to Section X3 (Provisions to Become Effective Following Designation) whereby the Common Test Scenarios Document is varied on it first becoming effective so that there are Service Requests that are deemed to be omitted from the document, then the following provisions shall apply:

(a) the Service Requests that are subject to such a direction shall, for so long as the variation in respect of that Service Request remains in effect, be "**Additional Release Services**";

(b) Parties that start User Entry Process Tests at a time where there are Additional Release Services shall undertake (and be able to successfully complete) the User Entry Process Tests without reference to those Additional Release Services;

(c) a User that completes User Entry Process Tests that did not include testing of Service Requests that used to be (but are no longer) Additional Release Services shall (notwithstanding any other provision of this Code) not be an Eligible User for those Service Requests until that User has successfully completed the applicable Additional SR Tests for those Service Requests; and

(d) "**Additional SR Tests**" means, in respect of one or more Service Requests that used to be (but are no longer) Additional Release Services, testing equivalent to User Entry Process Tests but undertaken only in respect of those Service Requests. Accordingly, and without limitation, the following shall apply:

(i) Additional SR Tests shall constitute a Testing Service, and shall therefore be subject to the provisions of Section H14 (Testing Services);

(ii) Additional SR Tests shall be provided by the DCC, and shall be capable of being undertaken by Parties, in accordance with Sections H14.12 to H14.21 (User Entry Process Tests), but:

(A) construed by reference to only those relevant Service Requests;

(B) where a Party has already demonstrated capability for the purposes of User Entry Process Tests, this can be relied upon for the purposes of the Additional SR Tests (unless the DCC considers that this is not appropriate for those Additional SR Tests);

(C) potentially (as provided for in the Common Test Scenarios Document) without the need to re-test the DCC Gateway Connection;

(D) without the need to re-test the Self-Service Interface; and

(E) subject to any other exceptions provided for in the Common Test Scenarios Document.

DCC Live Services Criteria Report

X1.18 This Section X1.18 shall apply where the DCC produces a report concerning its readiness to commence provision of the Services (or any part of the Services), and where the Secretary of State directs the Panel to review that report. Where this Section X1.18 applies, the Panel shall review the DCC's report and report to the Secretary of State in accordance with the criteria, scope and timing specified in the Secretary of State's direction.

Developing ETAD for RDP Entry Process Tests

X1.19 The DCC shall develop a revised Enduring Testing Approach Document which provides the detailed processes concerning the RDP Entry Process Tests in accordance with Section X1.20, such that the revised document can be re-designated pursuant to Section X5 (Incorporation of Certain Documents into this Code). The revisions shall include the following in respect of the RDP Entry Process Tests:

(a) entry criteria for RDPs wishing to undertake the tests;

(b) exit criteria demonstrating successful completion of the tests; and

(c) the process for first exchanging between the RDP and the DCC a full set of the Data to be exchanged under Section E2 (Provision of Data).

X1.20 The procedure by which the DCC is to develop the revisions to the Enduring Testing Approach Document is as follows:

(a) the DCC shall produce a draft by such date as the Secretary of State may direct;

(b) in producing the draft, the DCC must consult appropriately with Parties and other interested persons;

(c) where disagreements with the Parties arise concerning the proposed content of the draft, the DCC shall seek to reach an agreed solution with them, but without prejudice to the purposes of the document;

(d) having complied with (b) and (c) above, the DCC shall submit the draft revisions to the Secretary of State as soon as is reasonably practicable, and in any case by such date as the Secretary of State may direct;

(e) when submitting a draft under paragraph (d) above, the DCC shall indicate to the Secretary of State: (i) why the DCC considers the draft to be fit for purpose; (ii) copies of the consultation responses received; and (iii) any areas of disagreement that arose during the consultation process and that have not been resolved; and

(f) the DCC must comply with the requirements with respect to process, timeframe and/or further development of content in any direction that is given by the Secretary of State regarding the draft document.

X2. EFFECTIVE PROVISIONS AT DESIGNATION

Provisions to have Effect from Designation

X2.1 The Secretary of State shall be entitled to direct the Panel to cancel or suspend any Modification Proposal, in which case the Panel shall cancel or suspend the Modification Proposal in question and it shall not then be further progressed or implemented (or, in the case of suspension, shall not then be further progressed or implemented until the Secretary of State so directs).

X2.2 Where a Section is stated in this Section X2 to apply subject to more than one variation, then the Secretary of State may:

(a) designate different dates from which each such variation is to cease to apply; and/or

(b) designate a date from which one or more such variations are to cease to apply (without prejudice to the continued application of the other such variations).

X2.3 Before designating any dates for the purpose of this Section X2, the Secretary of State must consult the Authority, the Panel and the Parties in respect of the proposed date. Such consultation must allow such period of time as the Secretary of State considers appropriate in the circumstances within which to make representations or objections with respect to the proposed date. The requirement for consultation may be satisfied by consultation before, as well as after, the designation of this Code.

X3. PROVISIONS TO BECOME EFFECTIVE FOLLOWING DESIGNATION

Effective Dates

X3.1 Each Section, Schedule and SEC Subsidiary Document (or any part thereof) shall be effective, unless (at the time of a provision being added or modified by the Secretary of State pursuant to section 88 of the Energy Act 2008) the Secretary of State directs that such addition or modification is not to have effect, or is not to have an effect until a later date. Where the Secretary of State directs that an addition or modification is not to have effect, the Secretary of State may subsequently designate a date from which it is to have effect.

General

X3.2 Before designating any dates and/or making any directions for the purpose of this Section X3, the Secretary of State must consult the Authority, the Panel and the Parties in respect of the proposed date and/or the draft direction (as applicable). Such consultation must allow such period of time as the Secretary of State considers appropriate in the circumstances within which to make representations or objections with respect to the proposed date and/or the draft direction (as applicable).

X4. GOVERNANCE SET-UP ARRANGEMENTS

[NOT IN USE]

X5. INCORPORATION OF CERTAIN DOCUMENTS INTO THIS CODE

Smart Metering Equipment Technical Specifications

X5.1 The document designated by the Secretary of State, titled "Smart Metering Equipment Technical Specifications" and containing any one or more of the following:

(a) the ESME Technical Specification;

(b) the GSME Technical Specification;

(c) the IHD Technical Specification;

(d) the PPMID Technical Specification;

(e) the HCALCS Technical Specification; or

(f) the SAPC Technical Specification,

in accordance with Part G of Condition 22 of the DCC Licence shall, from the relevant date designated by the Secretary of State for the purpose of such document and of this Section X5.1, be incorporated in to this Code as the Schedule specified in such designation.

Communications Hub Technical Specifications

X5.2 The document designated by the Secretary of State as the Communications Hub Technical Specifications in accordance with Part G of Condition 22 of the DCC Licence shall, from the relevant date designated by the Secretary of State for the purpose of such document and this Section X5.2, be incorporated into this Code as the Schedule specified in such designation.

Certificate Policies

X5.3 Any document designated by the Secretary of State as a Certificate Policy in accordance with Part G of Condition 22 of the DCC Licence shall, from the relevant date designated by the Secretary of State for the purpose of such document and this Section X5.3, be incorporated into this Code as the Schedule or SEC Subsidiary Document specified in such designation.

Other Technical Specifications

X5.4 Each of the technical specifications and procedural or associated documents designated by the Secretary of State in accordance with Part G of Condition 22 of the DCC Licence shall, from the relevant date designated by the Secretary of State for the purpose of such document and this Section X5.4, be incorporated into this Code as the Schedule or SEC Subsidiary Document specified in such designation.

Re-Designation of Documents

X5.5 Paragraph 29(b) of Condition 22 of the DCC Licence includes a power for the Secretary of State to re-designate any document of a type referred to in Sections X5.1 to X5.4, subject to such amendments as he considers requisite or expedient. Where the Secretary of State exercises that power in relation to any such document:

(a) it shall be incorporated into this Code in substitution for the form of that document that was previously incorporated;

(b) the other provisions of this Section X5 shall apply to it as if it were a document being designated for the first time; and

(c) references in those provisions to the document being designated shall be read as referring to it being re-designated

Supplementary Provisions

X5.6 Paragraph 30 of Condition 22 of the DCC Licence includes a power for the Secretary of State to specify supplementary, incidental, consequential, governance or other provisions which are to have effect in this Code from the date designated for such purpose by the Secretary of State. This Code shall automatically be amended so as to include such provisions with effect from such date.

General

X5.7 This Code provides for the development of certain documents which may then be incorporated into this Code pursuant to this Section X5. Where this Code sets out the required purpose or content of such documents, the Secretary of State may designate for incorporation under this Section X5 documents that fulfil only part of that purpose or include only part of that content, with a view to subsequently re-designating more complete documents at a later date.

X5.8 The incorporation of documents into this Code pursuant to this Section X5 (and any provisions made pursuant to Section X5.6) shall not constitute a modification that should be subject to Section D (Modification Process). The incorporation of documents into this Code pursuant to this Section X5 (and any provisions made pursuant to Section X5.6) shall not constitute a variation of this Code that is time limited in accordance with Section X1.5A (and such documents and provisions shall remain part of this Code notwithstanding the deletion of this Section X5 in accordance with Section X1.5A).

X5.9 The documents incorporated into this Code pursuant to this Section X5 (and any provision made pursuant to Section X5.6) shall, from the date of their incorporation, be subject to modification in accordance with the provisions of this Code.

X5.10 Before designating any dates for the purpose of this Section X5, the Secretary of State must consult the Authority, the Panel and the Parties in respect of the proposed date. Such consultation must allow such period of time as the Secretary of State considers appropriate in the circumstances within which to make representations or objections with respect to the proposed date to be designated. The requirement for consultation may be satisfied by consultation before, as well as after, the designation of this Code.

X5.11 Before designating any date from which a document is to be incorporated into this Code pursuant to this Section X5, the content of such document must have been subject to such consultation as the Secretary of State considers appropriate in the circumstances (whether or not under this Code, whether or not undertaken by the Secretary of State and whether before or after the designation of this Code).

X6. TRANSITIONAL VARIATIONS

[NOT IN USE]

X7. TRANSITIONAL INCIDENT MANAGEMENT PROCEDURES

[NOT IN USE]

X8. DEVELOPING CH SUPPORT MATERIALS

[NOT IN USE]

X9. INTERIM DEVICE AND USER SYSTEM TESTING[1]

Interim Device Testing

X9.1 The DCC shall provide a testing service (referred to in this Section X9 as "**GFI Testing**") to enable eligible persons to test the interoperability of Devices (other than those comprising Communications Hubs) with the DCC Systems and with the Communications Hubs to be provided as part of the Testing Services, such that those Devices are able to respond to Commands received from or via the DCC in accordance with the requirements defined in the GB Companion Specification.

X9.2 The following shall apply in respect of GFI Testing:

(a) the following persons shall be eligible to undertake GFI Testing: Parties and persons that have signed agreements based on the Specimen Enabling Services Agreement (subject only to such variations from such specimen form as are reasonable in the circumstances, including so as to require compliance with this Section X9.2);

(b) the references in Section X9.1 to “Communications Hubs”, “DCC Systems” and “Devices” shall be interpreted as including reference to prototypes or simulations of those things (and GFI Testing shall not include communication via the SM WAN, or a simulation of the SM WAN);

(c) Section H14 (Testing Services) shall apply in respect of GFI Testing as if GFI Testing was a Testing Service, and the DCC and each person undertaking GFI Testing shall comply with Sections H14 in respect of GFI Testing as if GFI Testing was a Testing Service (provided that none of the following shall apply: Sections H14.3, H14.9, H14.10 and H14.11);

[1] This section X9 was included from 18 April 2016 as a variation under section X6 provisions.

(d) persons undertaking GFI Testing must each comply with such reasonable supplemental obligations as the DCC may notify to them from time to time (provided that such obligations are not inconsistent with the provisions of the Code that are in effect at that time); and

(e) the Testing Issue process in Section H14.37 to H14.45 (General: Testing Issue Resolution Process) shall not apply to GFI Testing, but the DCC must take reasonable steps to provide support and assistance to a person undertaking GFI Testing in order to assist that person in resolving Testing Issues encountered when undertaking GFI Testing.

Pre-UEPT Testing

X9.3 The DCC shall allow each Party that is entitled to use a DCC Gateway Connection to establish and validate a connection via that DCC Gateway Connection to a test environment to be used for the purposes of Pre-UEPT Testing.

X9.4 The DCC shall, with effect from 6 May 2016, provide a testing service (referred to in this Section X9 as " **Pre-UEPT Testing**") that enables Parties to test their capability (and that of their Systems) to undertake the following activities over a DCC Gateway Connection:

(a) the sending of (at least) the following Service Requests (which are identified by reference to the numbering used in the Common Test Scenarios Document):

(i) 4.1.1;

(ii) 5.1, 5.2 and 5.3;

(iii) 6.2.7, 6.11, 6.15.1, 6.15.2, 6.17, 6.20.1, 6.21 and 6.23;

(iv) 8.1.1, 8.2, 8.3, 8.4, 8.6, 8.7.1, 8.7.2, 8.8.1, 8.8.2, 8.9, 8.11, 8.12.1, 8.12.2, 8.13, 8.14.1, 8.14.2, 8.14.3 and 8.14.4; and

(v) 11.1, 11.2, 11.3, 12.1 and 12.2;

(b) the sending of one or more Signed Pre-Commands; and

(c) the receipt of Pre-Commands and Service Responses in respect of (at least) the Service Requests set out in paragraph (a) above (in the case of Pre-Commands, only to the extent those Service Requests are designed to generate Pre- Commands).

X9.5 From as soon as the DCC is reasonably able to do so, the DCC shall expand the Pre- UEPT Testing to include the ability of Parties to test their capability (and that of their Systems) to send each of the Service Requests identified in the Common Test Scenarios Document but not listed in Section X9.4(a).

X9.6 The following shall apply in respect of Pre-UEPT Testing:

(a) the references in Sections X9.4 and X9.5 to “Service Requests”, “Signed Pre- Commands”, “Pre-Commands”, “Service Responses”, “Device Alerts” and “DCC Alerts” shall be interpreted as including simulations of those things, which simulations may:

(i) include standardised or sample Data; and

(ii) omit Certificates, GBCS Payloads, Digital Signatures or Message Authentication Codes that would otherwise be required;

(b) Section H14 (Testing Services) shall apply in respect of Pre-UEPT Testing as if Pre-UEPT Testing was a Testing Service, and the DCC and each Party undertaking Pre-UEPT Testing shall comply with Sections H14 in respect of Pre-UEPT Testing as if Pre-UEPT Testing was a Testing Service (provided that none of the following shall apply: Sections H14.3, H14.4, H14.9 and H14.10);

(c) persons undertaking Pre-UEPT Testing must each comply with such reasonable supplemental obligations as the DCC may notify to them from time to time (provided that such obligations are not inconsistent with the provisions of the Code that are in effect at that time); and

(d) the Testing Issue process in Section H14.37 to H14.45 (General: Testing Issue Resolution Process) shall not apply to Pre-UEPT Testing, but the DCC must take reasonable steps to provide support and assistance to a Party undertaking Pre-UEPT Testing in order to assist that Party in resolving Testing Issues encountered when undertaking Pre-UEPT Testing.

Interaction with Device and User Systems Tests

X9.7 Not used.

X9.8 Not used.

X9.9 Not used.

X10. THRESHOLD ANOMALY DETECTION PROCEDURES

[NOT IN USE]

X11. SECRETARY-OF-STATE-LED VARIATIONS

Overview

X11.1 This Section X11 applies in respect of variations to this Code which the Secretary of State has the power to make under statute, Energy Licences and/or other provisions of this Code, and provides for a testing process to be followed in respect of such variations. References in this Section X11 to proposed variations includes variations which the Secretary of State is considering, is consulting on or has decided upon but not yet fully implemented.

Optional Analysis

X11.2 Where the Secretary of State so directs from time to time in respect of one or more proposed variations to this Code, the DCC shall analyse and report to the Secretary of State on the matters set out in that direction in accordance with the process and timescale set out in that direction. Such matters may include, without limitation:

(a) the extent to which changes would be required to the DCC Total System were the proposed variation to be made; and/or

(b) the likely development, capital and operating costs associated with such changes, and any consequential impact on the Charges.

SEC Variation Testing Approach Document

X11.3 Each SEC Variation Testing Approach Document is to be developed by the DCC pursuant to this Section X11, and then incorporated into this Code pursuant to Section X5 (Incorporation of Certain Documents into this Code).

X11.4 Where the Secretary of State so directs from time to time in respect of one or more proposed variations to this Code, the DCC shall develop a draft SEC Variation Testing Approach Document in respect of those proposed variations. The DCC shall develop that document in accordance with the timetable directed by the Secretary of State, in consultation with such other persons (if any) as the Secretary of State may direct, and otherwise in accordance with any process that the Secretary of State may direct.

X11.5 Each draft SEC Variation Testing Approach Document produced by the DCC shall set out the following in respect of the proposed variation(s), which must be consistent with any directions concerning the same made by the Secretary of State:

(a) the testing objectives;

(b) the testing to be undertaken;

(c) the testing environments to be used;

(d) the timetable for testing;

(e) the entry criteria for the start of testing or for the start of testing phases;

(f) the persons other than the DCC that are entitled or obliged to participate in testing;

(g) the entry criteria for the testing participants and the DCC;

(h) roles, responsibilities and obligations of the DCC and of the testing participants in respect of testing;

(i) the process for making amendments to the document, which shall include amendments directed by the Secretary of State;

(j) the process for resolving disputes under the document;

(k) the exit criteria for completion of testing (or stages of testing); and

(l) the process by which testing will be determined to be complete.

X11.6 The DCC shall submit each draft SEC Variation Testing Approach Document to the Secretary of State, indicating:

(a) why the DCC considers the draft to be fit for purpose;

(b) copies of the consultation responses received; and

(c) any areas of disagreement that arose during the consultation process and that have not been resolved, and, the DCC shall comply with any direction given by the Secretary of State to re-consider, re-consult and/or re-submit the draft document.

Compliance with SEC Variation Testing Approach Document

X11.7 The DCC and each person other than the DCC that participates in (or is required to participate in) testing under a SEC Variation Testing Approach Document shall comply with the SEC Variation Testing Approach Document.

X11.8 Section H14 (Testing Services) and the Enduring Testing Approach Document shall apply in respect of testing under a SEC Variation Testing Approach Document as if such testing was a Testing Service under Section H14.34 (Modification Implementation Testing); and each participant in such testing shall be deemed to be a Testing Participant for such purposes.

Z THE ALT HAN ARRANGEMENTS

All references to "Communications Hubs" in this Section Z are references to "SMETS2+ Communications Hubs".

Z1. THE ALT HAN FORUM

Establishment of the Alt HAN Forum

Z1.1 The Alt HAN Forum (the **Forum**) is hereby established.

Z1.2 The Forum shall:

(a) pursue the objectives, carry out the functions and have the powers set out in Sections Z1.3 to Z1.6;

(b) have the composition described in Sections Z1.7 to Z1.13;

(c) conduct its activities in accordance with the procedures set out in Sections Z1.14 to Z1.41;

(d) have the ability to establish, and to delegate its duties, powers and functions to, Sub-Groups in accordance with Sections Z1.42 to Z1.60,

and appeals from decisions of the Forum may be made to the Authority in accordance with Sections Z1.61 to Z1.67.

Forum Objectives, Functions and Powers

Forum Objectives

Z1.3 The Forum shall, in the performance of its functions and exercise of its powers, always act in a manner designed to achieve the objectives (the **Forum Objectives**) that:

(a) by virtue of the operation of this Section Z, Relevant Supplier Parties are able to comply with their obligations under Standard Conditions 55.2 and 55.16 of the Electricity Supply Licence and Standard Conditions 49.2 and 49.16 of the Gas Supply Licence;

(b) the Alt HAN Arrangements are given effect so as:

(i) to facilitate the economic and efficient carrying out of the Alt HAN Activities and provision of the Alt HAN Services;

(ii) to facilitate competition between persons engaged in, or in Commercial Activities connected with, the Supply of Energy;

(iii) to ensure that Energy Consumers' experience of the installation of Alt HAN Equipment at their premises is consistent with their reasonable expectations;

(iv) to ensure that all activities undertaken by or on behalf of Relevant Supplier Parties in relation to the installation, operation, maintenance, removal and replacement of Alt HAN Equipment are carried out in a fair, transparent, appropriate and professional manner;

(v) to ensure the protection of Data and the security of Data and Systems used for the purpose of the carrying out of the Alt HAN Activities and provision of the Alt HAN Services; and

(vi) to ensure that the Alt HAN Arrangements are administered in an economic, efficient and transparent manner; and

(c) the Forum conducts its affairs in an open and transparent manner.

Forum Functions

Z1.4 The Forum shall, in accordance with the provisions of this Section Z:

(a) make all decisions required for the purpose of:

(i) carrying out the Alt HAN Activities and the making available and provision of the Alt HAN Services, except for any decisions which may from time to time be delegated by it to AltHANCo or any Forum Sub- Group;

(ii) managing, maintaining, reviewing and updating the Exempt Premises List and any separate database of Exempt Premises, including reviewing and proposing to the Secretary of State revisions to the Exempt Premises List as required by Standard Condition 55.16 of the Electricity Supply Licence and Standard Condition 49.16 of the Gas Supply Licence.

(b) determine which (if any) decisions are to be delegated to AltHANCo or any Forum Sub-Group;

(c) give such directions to AltHANCo or any Forum Sub-Group as the Forum may consider appropriate (which may include directions in relation to any decisions otherwise delegated by the Forum);

(d) approve the annual budget of AltHANCo;

(e) determine any appeals made to it from decisions made by AltHANCo or a Forum Sub-Group; and

(f) make such other decisions as may from time to time be required in accordance with the provisions of this Section Z.

Z1.5 The Forum shall:

(a) provide to the Panel such report or other information as the Panel may request for the purpose of fulfilling its duty at Section C2.3(h) (Panel Duties); and

(b) (to the extent to which it reasonably considers that it is necessary to do so) liaise and exchange information with, provide advice to, and seek the advice of the Technical Architecture and Business Architecture Sub-Committee and the Security Sub-Committee on matters which fall within the scope of the activities of each of those Sub-Committees.

Forum Powers

Z1.6 Without prejudice to any other rights or powers granted to the Forum in this Section Z, the Forum shall, in accordance with the provisions of this Section Z, have the power to:

(a) make written representations in relation to the purpose or effect of any Draft Proposal or Modification Proposal which:

(i) is likely to affect this Section Z;

(ii) is likely to affect the provisions relating to the Alt HAN Charges at Section K (Charging Methodology);

(iii) relates to other parts of the Code, but may have a material effect on the Alt HAN Arrangements;

(b) appoint and remove professional advisers;

(c) consider, approve and authorise the entering into by AltHANCo of contracts; and

(d) do anything else necessary for, or reasonably incidental to, the fulfilment of its functions under this Section Z.

Forum Membership

Appointment of Members

Z1.7 Each Relevant Supplier Party:

(a) shall nominate one person to represent it in the Forum; and

(b) may at any time nominate a different person for that purpose, in replacement for any person previously nominated,

where all such nominations shall be made in writing to the Alt HAN Secretariat, and the Forum shall be composed of each of the persons (**Forum Members**) who are from time to time so nominated by the Relevant Supplier Parties.

Z1.8 A person may be nominated as a Forum Member by, may represent, and may vote on behalf of any two or more Relevant Supplier Parties (but shall not be entitled to exercise any rights to vote in such manner as to vote for more than one outcome in respect of any resolution).

Z1.9 Each Forum Member must be an individual, and cannot be a body corporate, association or partnership.

Election of Forum Chair and Alternate Chair

Z1.10 The Forum Members:

(a) shall, as the first item of business at the first meeting of the Forum, elect one person to serve as chair of the Forum (the **Forum Chair**) and one person to serve as alternate to the chair of the Forum (the **Alternate Chair**); and

(b) may at any subsequent time elect a different person to either role, in replacement for any person previously elected.

Z1.11 The Forum Chair and Alternate Chair may each be a Forum Member or any other person on whose appointment to such role the Forum is resolved.

Z1.12 The Forum may decide that the person elected as the Forum Chair (or, where that person is in employment, his or her employer) shall be compensated for such time as he or she spends performing the role of the Forum Chair in such amount, or at such rate, as the Forum may determine.

Z1.13 Notwithstanding the provisions of Section Z1.26, the election of a Forum Chair and Alternate Chair shall be by a simple majority vote of Forum Members present at the meeting at which that election takes place, each Forum Member being entitled to exercise a single vote.

Proceedings of the Forum

Meetings of the Forum

Z1.14 The Forum shall hold meetings with such frequency as it may determine or the Forum Chair may direct, but in any event shall meet as often as necessary in order to ensure the efficient performance of its functions, and at least once in every two month period.

Z1.15 The location and timing of each meeting shall be determined by the Forum or, where no such determination has been made, by the Forum Chair.

Z1.16 Forum Members may attend a meeting by telephone conference or other technological means (provided that each Forum Member attending the meeting acknowledges that he or she can communicate with each of the others).

Z1.17 Subject to the other provisions of this Section Z, the Forum may regulate the conduct of its meetings as it sees fit.

Alternates

Z1.18 Each Forum Member may, in each case by notice in writing to the Alt HAN Secretariat, appoint another person from time to time to act as his or her alternate.

Z1.19 Where a Forum Member does not attend a Forum meeting, his or her alternate shall be entitled to attend (and count, in the capacity of alternate, towards the quorum at) that meeting, and to exercise all of the functions and powers of the Forum Member at that meeting.

Z1.20 A person appointed as an alternate by any Forum Member:

(a) shall immediately cease to be an alternate if the appointing person ceases to be a Forum Member; and

(b) may be removed or replaced by that Forum Member from time to time, by notice in writing to the Alt HAN Secretariat.

Z1.21 A person may be appointed as an alternate by:

(a) a Forum Member who represents two or more Relevant Supplier Parties; or

(b) two or more Forum Members,

but in either case shall not be entitled to exercise any rights to vote in such manner as to vote for more than one outcome in respect of any resolution.

Z1.22 Unless the context otherwise requires, any reference in this Section Z to:

(a) a Forum Member shall be construed as including a reference to that Forum Member's alternate;

(b) the Forum Chair shall be construed as including, where the Forum Chair is unable to be available to perform his or her role, a reference to the Alternate Chair.

Quorum and Attendance of the Forum Chair

Z1.23 No decision may be made at any meeting of the Forum unless:

(a) that meeting is quorate, which shall be treated as being the case only if either:

(i) at least one half of all Forum Members nominated at that time are present at that meeting; or

(ii) the Forum Members who are present at that meeting are entitled to exercise at least two-thirds of the votes available to be cast; and

(b) the Forum Chair is present at that meeting.

Forum Chair

Z1.24 The Forum Chair shall preside at every meeting of the Forum and, if he or she is unable to attend any meeting, shall ensure that the Alternate Chair attends the meeting to act as Forum Chair.

Voting

Z1.25 Each Forum Member shall be entitled to attend, and to speak and vote, at every meeting of the Forum.

Z1.26 All decisions of the Forum shall be by resolution. Subject to Section Z1.13, in order for a resolution of the Forum to be passed at a meeting, a weighted majority of Forum Members present at that meeting must vote in favour of that resolution.

Z1.27 For these purposes:

(a) a number of votes shall be attributed to each Relevant Supplier Party in accordance with Sections Z1.28 to Z1.30 (the **Supplier Weighted Vote**); and

(b) each Forum Member shall be entitled to exercise a number of votes corresponding to the aggregate of the Supplier Weighted Votes of the Relevant Supplier Parties which that Forum Member represents.

Z1.28 Where one or more Supplier Parties have been notified by the DCC that Alt HAN Charges are payable in respect of all or any part of the Relevant Preceding Period, the Supplier Weighted Vote for each Relevant Supplier Party shall be calculated as follows:

$$SWV_p = \frac{AHC_{RPP}}{TAHC_{RPP}} \times 1000$$

Where:

$\mathrm{SWV_p}$ means the Supplier Weighted Vote for that Relevant Supplier Party;

AHC_{RPP} means the Alt HAN Charges that were payable by that Relevant Supplier Party in respect of the Relevant Preceding Period, as calculated by the DCC in accordance with the Charging Methodology;

$TAHC_{RPP}$ means the total amount of the Alt HAN Charges that were payable by all Relevant Supplier Parties in respect of the Relevant Preceding Period, as calculated by the DCC in accordance with the Charging Methodology.

Z1.29 Where the circumstances described in Section Z1.28 do not apply, the Supplier Weighted Vote for each Relevant Supplier Party shall be calculated as follows:

$$SWV_p = \frac{MPxN_p}{MPxN_{All\_p}} \times 1000$$

Where:

SWV_p	means the Supplier Weighted Vote for that Relevant Supplier Party;
$MPxN_p$	means the total number of MPANs and MPRNs related to Domestic Premises for which the Relevant Supplier Party was the Responsible Supplier at 24:00 on the last day of the Relevant Preceding Period;
$MPxN_{All\_p}$	means the sum of the values of MPxNp for all Relevant Supplier Parties.

Z1.30 For the purposes of Sections Z1.28 and Z1.29:

(a) in calculating the Supplier Weighted Vote, any fraction of a number of votes shall be rounded to the nearest whole number (and 0.5 of a vote shall be rounded upwards);

(b) the Supplier Weighted Vote shall never have a value less than 1 (one);

(c) the **Relevant Preceding Period** shall be:

(i) in relation to any vote at a Forum meeting taking place in the period between 16 May and 15 November (inclusive) in any year, the month of April falling immediately prior to the start of that period; and

(ii) in relation to any vote at a Forum meeting taking place in the period between 16 November in any year and 15 May in the following year, the month of October falling immediately prior to the start of that period; and

(d) any information provided by the DCC for the purposes of calculating the Supplier Weighted Vote shall be deemed to be accurate unless and until the contrary is proved.

Z1.31 A resolution put to a vote at a Forum meeting shall be passed if the number of votes in favour of that resolution correspond to more than 50% of the total number of votes which all Forum Members attending that meeting are entitled to exercise.

Z1.32 The voting process, counting of votes, and calculation of Supplier Weighted Votes in respect of all resolutions which are required to be passed by a weighted majority of Forum Members shall take place in accordance with the Forum Voting Protocol. The Forum Voting Protocol may specify obligations on the DCC or any Party to provide information, or otherwise take any steps, for the purpose of facilitating that process, count or calculation.

Meeting Notice and Papers

Z1.33 Each meeting that the Forum determines, or the Forum Chair directs, is to be held shall be convened by the Alt HAN Secretariat. Such meeting shall be convened on at least 5 Working Days' advance notice (or such shorter period as the Forum may approve). Such notice shall be given to:

(a) each of the Forum Members (and any appointed alternates);

(b) each of the persons referred to in Section Z1.37; and

(c) each of the Relevant Supplier Parties.

Z1.34 The notice of each Forum meeting shall contain or be accompanied by a statement of the following:

(a) the time, date and location of the meeting;

(b) the arrangements for those wishing to attend the meeting by telephone conference or other technological means; and

(c) an agenda and any supporting papers.

Z1.35 The agenda for each Forum meeting shall include any such matters as:

(a) the Forum has determined;

(b) the Forum Chair has directed, or

(c) any two or more Relevant Supplier Parties (not being Parties which have the same ultimate holding company) have requested for inclusion.

Z1.36 The proceedings of a Forum meeting shall not be invalidated by the accidental omission to give notice of the meeting to (or non-receipt of that notice by) any person entitled to receive it.

Attendance by Other Persons

Z1.37 One representative from each of the following persons shall be entitled to attend and speak (but not vote) at any meeting of the Forum:

(a) the Secretary of State;

(b) the Authority; and

(c) any other person that the Forum determines, or the Forum Chair directs, should be invited to attend.

Z1.38 The Forum Chair may (at his or her discretion on grounds of confidentiality) exclude from any part of a Forum meeting any person admitted pursuant to Section Z1.37(c).

Minutes of Forum Meetings

Z1.39 The Alt HAN Secretariat shall, within 10 Working Days of each Forum meeting, circulate copies of the minutes of that meeting to each of the Forum Members, the Secretary of State and the Authority.

Z1.40 If any Forum Member, the Secretary of State or the Authority disagrees with any item in the minutes, he or she shall at the next Forum meeting notify the Forum Chair of the matters which are the cause of the disagreement, and those matters shall be discussed at that meeting.

Z1.41 The Alt HAN Secretariat shall maintain a record of all resolutions voted on by the Forum, which shall indicate how each Forum Member voted on each resolution and (where applicable) what voting share was attributable to that Forum Member at that meeting, and shall make such record available on request to any Relevant Supplier Party, the Secretary of State and the Authority.

Forum Sub-Groups

Establishing Forum Sub-Groups

Z1.42 The Forum may establish committees (**Forum Sub-Groups**) for the purposes of doing or assisting the Forum in doing anything to be done by the Forum pursuant to this Section Z.

Z1.43 The Forum may establish a Forum Sub-Group on a standing basis or for a fixed period or a finite purpose.

Z1.44 The Forum may decide that any Forum Sub-Group is to be dissolved.

Z1.45 The Forum may delegate to any Forum Sub-Group such of the duties, powers and functions of the Forum as the Forum may specify.

Membership of Forum Sub-Groups

Z1.46 Each Forum Sub-Group shall be composed of such persons of suitable experience and qualifications as the Forum shall decide and as are willing to serve thereon (**Forum Sub-Group Members**), which may include any Forum Member.

Z1.47 Each Forum Sub-Group Member must be an individual, and cannot be a body corporate, association or partnership.

Z1.48 Before establishing any Forum Sub-Group, the Forum shall invite (by such means as it considers appropriate) applications from individuals who wish to serve on the Forum Sub-Group.

Z1.49 Once a Forum Sub-Group has been established, the Forum may admit such additional persons as Forum Sub-Group Members, or remove any person from being a Forum Sub-Group Member, as the Forum considers appropriate (including on the application of any Relevant Supplier Party or any existing Forum Sub-Group Member).

Z1.50 Each Forum Sub-Group Member shall, when acting in that capacity:

(a) act independently, not as a delegate, and without undue regard to the interests of any Related Person; and

(b) act in a manner designed to facilitate the performance by the Forum of its duties under this Section Z.

Z1.51 Each person appointed as a Forum Sub-Group Member must confirm in writing to the Alt HAN Secretariat (for the benefit of AltHANCo and each Relevant Supplier Party) that that person:

(a) agrees to act as a Forum Sub-Group Member in accordance with this Section Z, including the requirements of Section Z1.50; and

(b) will be available as reasonably required throughout his or her term of office both to attend Forum Sub-Group meetings and to undertake work outside those meetings as may reasonably be required.

Z1.52 The Forum may, either generally or in relation to specific cases, approve:

(a) the payment to a Forum Sub-Group Member (or, where that person is in employment, his or her employer) of compensation for such time as he or she spends performing the role of a Forum Sub-Group Member; and

(b) the amount, rate, or means of calculation of such payment.

Terms of Reference and Procedure of Forum Sub-Groups

Z1.53 The Forum shall set out in writing any such duties, powers and functions of the Forum as it has delegated to each Forum Sub-Group.

Z1.54 The Forum shall specify in writing the terms of reference and procedural rules that are to be followed by each Forum Sub-Group (which may be revised from time to time by the Forum).

Z1.55 Save to the extent otherwise specified by the Forum, a Forum Sub-Group shall conduct its business in such manner as it considers appropriate.

Z1.56 No Forum Sub-Group may delegate any of its duties, powers or functions unless it has been expressly authorised to do so by the Forum.

Z1.57 Any resolutions of a Forum Sub-Group shall:

(a) only have binding effect as a decision of the Forum if the Forum has formally delegated the required decision-making power to that Forum Sub-Group; and

(b) within 10 Working Days of the date of the resolution be notified by the Forum Sub-Group, by means of the Alt HAN Secretariat, to each Relevant Supplier Party.

Appeals from Decisions of a Forum Sub-Group

Z1.58 A Relevant Supplier Party may appeal to the Forum any decision of a Forum Sub-Group which otherwise has binding effect as a decision of the Forum.

Z1.59 An appeal under Section Z1.58 will only be validly made if it is notified to the Alt HAN Secretariat within 20 Working Days of the date on which the Forum Sub-Group made the decision which is subject to appeal.

Z1.60 Where a decision of a Forum Sub-Group is appealed:

(a) the decision shall be treated as having no effect; and

(b) the Forum shall make the decision afresh, which shall then have effect for the purposes of this Section Z in substitution for the decision of the Forum Sub- Group.

Appeals from Decisions of the Forum

Z1.61 A Relevant Supplier Party may appeal to the Authority any decision of the Forum on the ground that it is inconsistent with the Forum Objectives.

Z1.62 An appeal under Section Z1.61 will only be validly made if:

(a) it is notified to the Authority within 30 Working Days of the date on which the Forum made the decision which is subject to appeal;

(b) a copy of the notice is given to the Alt HAN Secretariat on the same date on which it is sent to the Authority; and

(c) the notice specifies why the Relevant Supplier Party which is bringing the appeal considers that the decision which is subject to appeal is inconsistent with the Forum Objectives.

Z1.63 Where the Alt HAN Secretariat is notified of an appeal, it shall arrange for a copy of the notice of appeal to be provided to all Relevant Supplier Parties.

Z1.64 The Authority may adopt such process and procedure as it thinks fit in relation to the determination of any appeal, and may give interim directions as to the effect of the decision being appealed prior to the appeal being determined.

Z1.65 The Forum shall provide such information, support and assistance to the Authority in relation to the determination of any appeal as the Authority may reasonably request.

Z1.66 Where the Authority considers that the Relevant Supplier Party which brought the appeal:

(a) has failed to establish that the decision being appealed is inconsistent with the Forum Objectives, it shall uphold the decision; or

(b) has established that the decision being appealed is inconsistent with the Forum Objectives, it may:

(i) quash the decision;

(ii) remit the decision to be remade by the Forum; and/or

(iii) substitute its own decision for that of the Forum, which shall then have effect for the purposes of this Section Z as if it had been a decision of the Forum.

Z1.67 Any decision of the Authority in relation to a matter appealed to it under Section Z1.61 shall be final and binding for the purposes of this Section Z.

Z2. THE ALT HAN COMPANY

Establishment of AltHANCo

Z2.1 The Alt HAN Company (**AltHANCo**) shall be established in accordance with the Annex to this Section Z.

Z2.2 AltHANCo shall act as a corporate vehicle in relation to the business of the Forum, including entering into any contractual arrangements in order to give effect to any resolution of the Forum which it is necessary or desirable to implement by means of a binding contract.

Z2.3 AltHANCo shall pursue the objectives, fulfil the duties and have the powers set out in Sections Z2.5 to Z2.7, and all decisions on behalf of AltHANCo shall be made by the board of directors of AltHANCo (the **Board**).

Z2.4 The Board shall:

(a) have the membership described in Sections Z2.8 to Z2.22; and

(b) conduct its activities in accordance with the procedures set out in Sections Z2.23 to Z2.45,

and appeals from decisions of the Board may be made to the Forum in accordance with Sections Z2.46 to Z2.48.

AltHANCo Objectives, Duties and Powers

AltHANCo Objectives

Z2.5 AltHANCo shall, in the discharge of its duties and exercise of its powers, always act in a manner designed to achieve the objectives (the **AltHANCo Objectives**) that:

(a) the Forum Objectives are achieved;

(b) this Section Z is given effect in a fair manner without undue discrimination between the Relevant Supplier Parties or classes of Relevant Supplier Party; and

(c) AltHANCo conducts its affairs in an open, transparent and efficient manner.

AltHANCo Duties

Z2.6 AltHANCo shall, in accordance with the provisions of this Section Z:

(a) make all such decisions as may be delegated to it from time to time by the Forum;

(b) undertake such activities as are necessary for the purpose of giving effect to the decisions of the Forum;

(c) comply with any directions given to it by the Forum; and

(d) undertake such other activities and make such other decisions as may from time to time be required in accordance with the provisions of this Section Z.

AltHANCo Powers

Z2.7 Without prejudice to any other rights or powers granted to AltHANCo in this Section Z, AltHANCo shall, in accordance with the provisions of this Section Z, have the power:

(a) where the Forum has so resolved, to pay compensation to the Forum Chair (or to his or her employer) for such time as he or she spends performing the role of the Forum Chair in such amount, or at such rate, as the Forum has determined;

(b) where the Forum has approved the payment of compensation to any Forum Sub- Group Member (or his or her employer) for time spent performing the role of a Forum Sub-Group Member, to pay compensation to that Forum Sub-Group Member (or his or her employer) in such amount, at such rate or in accordance with such means of calculation as the Forum has approved;

(c) to appoint and remove professional advisers;

(d) to enter into contracts; and

(e) to do anything else necessary for, or reasonably incidental to, the discharge of its duties under this Section Z.

Board Membership

Board Composition

Z2.8 The Board shall be composed of no fewer than three persons (each a **Board Member**).

Z2.9 Each Board Member must be an individual, and cannot be a body corporate, association or partnership.

Election of Board Members

Z2.10 The first Board Members to be appointed shall be the persons elected following an election process administered by the Secretary of State prior to this Section Z coming into effect.

Z2.11 Of the persons appointed in accordance with Section Z2.10:

(a) one of them shall retire 12 months after this Section Z comes into effect; and

(b) two of them shall retire 24 months after this Section Z comes into effect,

as specified by the Secretary of State in a notice informing them of their appointment as Board Members following the election process referred to in that Section.

Z2.12 Each Board Member shall serve as such until his or her retirement in accordance with Section Z2.16 or resignation or removal in accordance with Sections Z2.17 and Z2.18.

Z2.13 The Board shall produce, and submit to the Forum, the draft of a document setting out the process by which Board Members are to be elected following the retirement, resignation or removal of those appointed in accordance with Section Z2.10.

Z2.14 The Forum:

(a) shall, subject to such amendments as it may determine, adopt the document produced by the Board which (in the form in which it is adopted) shall be known as the **AltHANCo Election Protocol** ; and

(b) may from time to time determine to modify the AltHANCo Election Protocol in such manner as it may consider appropriate.

Z2.15 The election of Board Members following the retirement, resignation or removal of those appointed in accordance with Section Z2.10 shall be conducted in accordance with the version of the AltHANCo Election Protocol which is in effect at that time.

Retirement of Board Members

Z2.16 Subject to earlier resignation or removal from office in accordance with Sections Z2.17 and Z2.18, and without prejudice to his or her ability to stand for re-election, each Board Member shall retire (at which point his or her office shall become vacant) as follows:

(a) a Board Member appointed in accordance with Section Z2.10 shall retire in accordance with the terms of the appointment specified by the Secretary of State under Section Z2.11; and

(b) a Board Member appointed following a subsequent election shall retire 24 months after that appointment took effect.

Resignation and Removal of Board Members

Z2.17 A Board Member may:

(a) resign his or her office on giving 10 Working Days' notice in writing to the Alt HAN Secretariat;

(b) be removed from office by the AltHANCo Chair on notice to the Alt HAN Secretariat if the Board Member fails to attend in person at least half of the Board meetings held in any period of 12 months; or

(c) be removed from office by the other Board Members (acting unanimously) on notice to the Alt HAN Secretariat if those other Board Members consider that he or she is in breach of the confirmation that was given in accordance with Section Z2.20.

Z2.18 A Board Member shall automatically be removed from office if he or she:

(a) dies;

(b) is admitted to hospital in pursuance of an application under the Mental Health Act 1983 or the Mental Health (Care and Treatment) (Scotland) Act 2003, or an order is made by a court with competent jurisdiction in matters concerning mental disorder for his detention or for the appointment of a receiver, curator bonis or other person with respect to his or her property or affairs;

(c) becomes bankrupt or makes any arrangement or composition with his or her creditors;

(d) becomes prohibited by law from being a director of a company under the Companies Act 2006; or

(e) is convicted of an indictable criminal offence.

Duties of Board Members

Z2.19 A person appointed as a Board Member, when acting in that capacity, shall:

(a) act independently, not as a delegate, and without undue regard to the interests of any Related Person;

(b) exercise reasonable skill and care to the standard reasonably expected of a director of a company under the Companies Act 2006; and

(c) act in a manner designed to facilitate the performance by AltHANCo of its duties under this Section Z.

Board Member Confirmation

Z2.20 Each person elected as a Board Member must confirm in writing to the Alt HAN Secretariat (for the benefit of AltHANCo and each Relevant Supplier Party) that that person:

(a) agrees to act as a Board Member in accordance with this Section Z, including the requirements of Section Z2.19;

(b) agrees to accept appointment as a director of AltHANCo, and to act in such capacity in accordance with this Section Z; and

(c) will be available as reasonably required throughout his or her term of office both to attend Board meetings and to undertake work outside those meetings as may reasonably be required,

and must further complete any and all forms required to be completed by law in order for that person to become a director of AltHANCo.

Z2.21 The appointment of a person who would otherwise be a Board Member shall lapse (and the relevant office shall become vacant) if that person does not comply with the requirements of Section Z2.20 within 20 Working Days after a request from the Alt HAN Secretariat to do so.

Notification of Related Persons

Z2.22 Each Board Member shall, as soon as reasonably practicable after his or her election and upon any later relevant change in circumstance, disclose in writing to the Alt HAN Secretariat, the name of each Related Person who is a Relevant Supplier Party or is otherwise likely to be materially affected by the Alt HAN Arrangements (other than in the capacity of Energy Consumer).

Proceedings of the Board

Appointment of the Chair

Z2.23 The Board Members:

(a) shall, as the first item of business at the first meeting of the Board, elect from among them one person to serve as chair of AltHANCo (the **Chair**); and

(b) may at any subsequent time elect from among them a different person for that purpose, in replacement for any person previously elected.

Meetings of the Board

Z2.24 The Board shall hold meetings with such frequency as it may determine or the Chair may direct, but in any event shall meet as often as necessary in order to ensure the efficient discharge of its duties, and at least once in every two month period.

Z2.25 The location and timing of each meeting shall be determined by the Board or, where no such determination has been made, by the Chair.

Z2.26 Board Members may attend a meeting by telephone conference or other technological means (provided that each Board Member attending the meeting acknowledges that he or she can communicate with each of the others).

Z2.27 Subject to the other provisions of this Section Z (including the Annex), the Board may regulate the conduct of its meetings as it sees fit.

Alternates

Z2.28 The Chair shall, and each other Board Member may, in each case by notice in writing to the Alt HAN Secretariat, appoint another person from time to time to act as his or her alternate.

Z2.29 Where a Board Member does not attend a Board meeting, his or her alternate shall be entitled to attend (and count, in the capacity of alternate, towards the quorum at) that meeting, and to exercise all of the functions and powers of the Board Member at that meeting.

Z2.30 A person appointed as an alternate by any Board Member:

(a) shall immediately cease to be an alternate if the appointing person ceases to be a Board Member; and

(b) may be removed or replaced by that Board Member from time to time, by notice in writing to the Alt HAN Secretariat.

Z2.31 Unless the context otherwise requires, any reference in this Section Z to a Board Member shall be construed as including a reference to that Board Member's alternate.

Quorum

Z2.32 No decision may be made at any meeting of the Board unless a quorum is present, and the quorum at each meeting of the Board shall be two, at least one of whom must be the Chair.

The Chair

Z2.33 The Chair shall preside at every meeting of the Board and, if he or she is unable to attend any meeting, shall ensure that his or her alternate attends the meeting to act as Chair.

Voting

Z2.34 Each Board Member shall be entitled to attend, and to speak and vote, at every meeting of the Board.

Z2.35 All decisions of the Board shall be by ordinary resolution, passed by a simple majority of Board Members present at the meeting at which the vote takes place.

Z2.36 For these purposes the Chair shall be entitled to vote, and if the votes are tied shall have a second and casting vote.

Meeting Notice and Papers

Z2.37 Each meeting that the Board determines, or the Chair directs, is to be held shall be convened by the Alt HAN Secretariat. Such meeting shall be convened on at least 5 Working Days' advance notice (or such shorter period as the Board may approve). Such notice shall be given to:

(a) each of the Board Members (and any appointed alternates);

(b) each of the persons referred to in Section Z2.40; and

(c) each Relevant Supplier Party.

Z2.38 The notice of each Board meeting shall contain or be accompanied by a statement of the following:

(a) the time, date and location of the meeting;

(b) the arrangements for those wishing to attend the meeting by telephone conference or other technological means; and

(c) an agenda and any supporting papers.

Z2.39 The proceedings of a Board meeting shall not be invalidated by the accidental omission to give notice of the meeting to (or non-receipt of that notice by) any person entitled to receive it.

Attendance by Other Persons

Z2.40 One representative from each of the following persons shall be entitled to attend and speak (but not vote) at any meeting of the Board:

(a) the Secretary of State;

(b) the Authority; and

(c) any other person that the Board determines, or the Chair directs, should be invited to attend.

Z2.41 Any Relevant Supplier Party shall be entitled to send a representative to attend a Board meeting provided that the Relevant Supplier Party gives the Alt HAN Secretariat notice of its intention to do so at least 3 Working Days' notice in advance of that meeting (or such shorter period of notice as the Chair may approve). Such a representative shall be entitled to attend and (at the Chair's invitation) speak (but in no circumstances vote) at the meeting.

Z2.42 The Chair may (at his or her discretion on grounds of confidentiality) exclude from any part of a Forum meeting any person admitted pursuant to Section Z2.40(c).

Minutes of Board Meetings

Z2.43 The Alt HAN Secretariat shall, within 10 Working Days of each Board meeting, circulate copies of the minutes of that meeting to each of the Board Members, each Relevant Supplier Party, the Secretary of State and the Authority.

Z2.44 If any Board Member disagrees with any item in the minutes, he or she shall at the next Board meeting notify the Chair of the matters which are the cause of the disagreement, and those matters shall be discussed at that meeting.

Z2.45 The Alt HAN Secretariat shall maintain a record of all resolutions voted on by the Board, which shall indicate how each Board Member voted on each resolution, and shall make such record available on request to any Relevant Supplier Party.

Appeals from Decisions of the Board

Z2.46 A Relevant Supplier Party may appeal to the Forum any decision of the Board.

Z2.47 An appeal under Section Z2.46 will only be validly made if it is notified to the Alt HAN Secretariat within 20 Working Days of the date on which the Board made the decision which is subject to appeal.

Z2.48 Where a decision of the Board is appealed:

(a) the decision shall be treated as having no effect; and

(b) the Forum shall make the decision afresh, which shall then have effect for the purposes of this Section Z in substitution for the decision of the Board.

Z2.49 Where personnel of AltHANCo (or its contractor) reasonably require, in connection with the Alt HAN Activities, access to a premises (or part of a premises) to which members of the public do not generally have free access, then:

(a) each Relevant Supplier Party agrees that these personnel may identify themselves as a representative of the Relevant Supplier Parties when seeking to obtain verbal permission from a relevant Energy Consumer to access such premises or part of a premises (for which purpose, a "relevant Energy Consumer" is one of the Relevant Supplier Party's Energy Consumers who reasonably appears to have authority to grant such permission);

(b) subject to obtaining such permission from a relevant Energy Consumer, these personnel may access such premises or part of a premises as the Relevant Supplier Party's representative for purposes connected to the Alt HAN Activities;

(c) AltHANCo shall ensure that these personnel shall, while attending the premises of Energy Consumers in connection with the Alt HAN Activities, act in accordance with Good Industry Practice, the site rules and reasonable instructions of the owner and/or occupier of the relevant premises notified to such personnel, and all Laws and/or Directives applicable to representatives of Relevant Supplier Parties when attending premises;

(d) AltHANCo shall ensure that each Relevant Supplier Party has the right under the Contract (Rights of Third Parties) Act 1999 to enforce breaches of paragraph (c) above against AltHANCo's contractor in accordance with AltHANCo's contract with such contractor; and

(e) AltHANCo shall ensure that the personnel who attend the premises of Energy Consumers pursuant to this Section Z2.49 are subject to such reasonable vetting, and comply with such reasonable consumer protection measures, as the Forum may determine from time to time.

Z3. ALT HAN SECRETARIAT

Z3.1 AltHANCo shall, from time to time, appoint and remove, or make arrangements for the appointment and removal of, one or more persons to be known as the **Alt HAN Secretariat**.

Z3.2 The Alt HAN Secretariat shall perform those tasks and functions expressly ascribed to it under this Section Z, and any other tasks and functions that either the Forum or AltHANCo may assign to it from time to time. In particular, the Alt HAN Secretariat shall:

(a) support the election of Board Members in accordance with the provisions of the AltHANCo Election Protocol;

(b) support the voting of Forum Members in accordance with the Forum Voting Protocol;

(c) provide such other support to the proceedings of the Forum, any Forum Sub-Group and the Board as each of them may respectively require; and

(d) provide or procure such facilities and services in connection with the operation of the Forum, any Forum Sub-Group and the Board as each of them may respectively require.

Z3.3 AltHANCo shall be responsible for ensuring that the Alt HAN Secretariat undertakes its tasks and functions in respect of this Section Z. In particular, AltHANCo shall ensure that the arrangements under which the Alt HAN Secretariat is appointed oblige it to undertake such tasks and functions on terms no less onerous than those provided for by this Code.

Z3.4 Subject to the other requirements of this Section Z3, the Alt HAN Secretariat shall be appointed by AltHANCo on such terms and conditions and in return for such remuneration as AltHANCo sees fit.

Z3.5 The person appointed as the Alt HAN Secretariat may be the person appointed to carry out the role of Code Administrator and/or the Secretariat.

Z4. ALT HAN COSTS AND BUDGETS

General

Z4.1 The costs and expenses incurred by (or on behalf of) the Forum in exercising its powers, performing its functions and discharging its duties in respect of this Section Z shall be incurred by AltHANCo, and the DCC shall provide AltHANCo:

(a) with the funds necessary to meet such costs and expenses; and

(b) with the funds necessary to meet all other costs and expenses incurred by AltHANCo in the exercise of its duties, powers and functions under this Section Z.

Alt HAN Costs and Expenses

Z4.2 The costs and expenses capable of recovery under this Section Z4 (the **Alt HAN Costs**) shall be all the reasonable costs and expenses incurred:

(a) subject to Section Z4.3, by the Forum Chair, Alternate Chair, Forum Members, Board Members and Forum Sub-Group Members in their capacities as such;

(b) by AltHANCo under or in connection with contracts that AltHANCo has entered into in accordance with this Section Z, including in particular any contracts for:

(i) the acquisition of any services which comprise or form a part of the Alt HAN Activities;

(ii) the provision of any Alt HAN Services;

(iii) the appointment of the Forum Chair;

(iv) the appointment of Forum Sub-Group Members;

(v) the appointment of the Alt HAN Secretariat; and

(vi) the appointment of advisers;

(c) by AltHANCo under or in connection with the DAB Phase Financing (the "**DAB Phase Financing Alt HAN Costs**");

(d) by AltHANCo under or in connection with the Roll Out Phase Financing (the "**Roll Out Financing Alt HAN Costs**"); and

(e) by AltHANCo under or in connection with any provision of this Section Z,

(in each case) provided that such costs or expenses are provided for in, or otherwise consistent with, an Approved Alt HAN Budget or an Approved Alt HAN Financing Budget.

Z4.3 Subject to the terms of those contracts referred to in Section Z4.2(b):

(a) the Forum Chair, Alternate Chair, Forum Members, Board Members and Forum Sub-Group Members shall be entitled to recover all reasonable travel expenses properly incurred by them in their roles as such (and the Board shall adopt a policy that sets out guidelines regarding what constitutes reasonable travel expenses);

(b) no Alternate Chair, Forum Member or Board Member shall be entitled to a salary in respect of his or her role as such, or to any payment in respect of the time he or she spends in performing that role; and

(c) no Forum Sub-Group Member shall be entitled to a salary in respect of his or her role as such, or to any payment in respect of the time he or she spends in performing that role, except to the extent that the Forum has approved any such payment.

Z4.4 Where the Forum Chair, Alternate Chair or any Forum Member, Board Member or Forum Sub-Group Member wishes to recover any cost or expense (excepting, in the case of the Forum Chair, any regular payment of salary for which no claim is required to be made) he or she shall submit evidence of the cost or expense in question to the Board (or a named person approved by the Board) for approval.

Z4.5 Any cost or expenses referred to in Section Z4.4 shall only be approved to the extent that it is an Alt HAN Cost, and only if the evidence is submitted in a timely manner (and in any event on or before the 20th Working Day following the end of the relevant Regulatory Year). Once approved, the evidence of the Alt HAN Cost shall be submitted to AltHANCo for payment.

Z4.6 Within 20 Working Days following receipt of evidence of an Alt HAN Cost that has been approved in accordance with Section Z4.5, AltHANCo shall pay the relevant amount to the Forum Chair, Alternate Chair, Forum Member, Board Member or Forum Sub-Group Member making the claim.

Alt HAN Costs to be Reimbursed by the DCC

Z4.7 The Alt HAN Costs incurred by AltHANCo shall be reimbursed to AltHANCo by the DCC. Nothing in Section M2 (Limitations of Liability) shall limit the DCC's liability to reimburse AltHANCo for the AltHANCo Costs.

Z4.8 AltHANCo may periodically invoice the DCC for the Alt HAN Costs incurred, or reasonably expected to be incurred, by AltHANCo in accordance with the Approved Alt HAN Budget or Approved Alt HAN Financing Budget, provided that AltHANCo shall deduct from such invoice any amounts that represent previous overpayments by the DCC (due to the inaccuracy of AltHANCo estimates, or otherwise) on the basis that AltHANCo shall:

(a) only deduct from an invoice for DAB Phase Financing Alt HAN Costs any previous overpayment in respect of a DAB Phase Financing Alt HAN Cost; and

(b) only deduct from an invoice for Roll Out Financing Alt HAN Costs any previous overpayment in respect of a Roll Out Financing Alt HAN Cost.

Z4.9 The DCC shall pay each invoice submitted by AltHANCo in accordance with Section Z4.7 within 10 Working Days of receipt of such invoice by the DCC, to the account or accounts for payment specified by AltHANCo to the DCC from time to time.

Z4.10 It is acknowledged that the DCC is entitled to recover amounts paid by it to AltHANCo in accordance with this Section Z4 through the Charges (subject to the requirements of the DCC Licence).

Z4.11 In the event that the DCC does not pay AltHANCo in accordance with Section Z4.9, and subject to prior approval from the Authority, AltHANCo may invoice the Relevant Supplier Parties for the unpaid amount (and those Parties shall pay the invoiced amounts to AltHANCo as if they were Charges).

Z4.12 Where Section Z4.11 applies, the amount to be paid by each Relevant Supplier Party shall, unless the Authority approves or directs the use of an alternative methodology, be the same as the amount that the Relevant Supplier Party would have paid in Fixed Alt HAN Charges and in Explicit Charges under Section K7.6(j), calculated in accordance with the Charging Methodology, had the amounts been recovered by the DCC through the Charges.

Z4.13 Any amounts paid by a Relevant Supplier Party in accordance with Section Z4.12 shall be reimbursed by AltHANCo to that Relevant Supplier Party (plus interest at the Non- Default Interest Rate) at such time as the Authority may determine.

Budgets and Work Plans

Timetable

Z4.14 The Board shall take all reasonable steps to give effect to the provisions of Sections Z4.15 to Z4.19 so that a copy of each Approved Alt HAN Budget is provided to the DCC by no later than 1 December in the year prior to the commencement of the first Regulatory Year to which that Approved Alt HAN Budget relates.

Draft Budgets and Work Plans

Z4.15 The Board shall during each Regulatory Year prepare and circulate to all Relevant Supplier Parties, the Secretary of State and the Authority a draft budget in respect of Alt HAN Costs for the next two Regulatory Years commencing thereafter (a **Draft Alt HAN Budget**).

Z4.16 Each Draft Alt HAN Budget:

(a) shall set out the Board's good-faith estimate of the Alt HAN Costs that it anticipates will be incurred (or committed to) during each of the relevant Regulatory Years (but excluding DAB Phase Financing Alt HAN Costs and Roll Out Financing Alt HAN Costs to the extent that the Board is satisfied those costs are or will be covered by a separate budget as contemplated under Section Z4.17A);

(b) shall set out how that estimate is composed of the Board's estimates of the total costs and expenses that it anticipates will be incurred (or committed to) during each of the relevant Regulatory Years in relation to:

(i) the carrying out of the Alt HAN Activities;

(ii) the provision of Alt HAN Services in respect of:

(A) installed Shared Solution Alt HAN Equipment;

(B) installed Point-to-Point Alt HAN Equipment; and

(C) Point-to-Point Alt HAN Equipment that has been provided to a Party, but has not yet been installed by or on behalf of a Relevant Supplier Party;

(c) shall be accompanied by a detailed work plan showing the activities and projects to which the relevant costs and expenses relate; and

(d) may make reasonable provision for contingencies.

Z4.17 Each Draft Alt HAN Budget must provide for limits (both individually and in the aggregate) on costs and expenses not expressly provided for in the budget which can be incurred without having to amend the budget.

Z4.17A The Board may prepare and circulate to all Relevant Supplier Parties, the Secretary of State and Authority separate budgets in respect of:

(a) the DAB Phase Financing Alt HAN Costs (a **Draft Alt HAN (DAB Phase) Financing Budget**); and

(b) the Roll Out Financing Alt HAN Costs (a **Draft Alt HAN (Roll Out) Financing Budget).**

Z4.17B Each Draft Alt HAN Financing Budget that the Board decides to prepare and circulate:

(a) shall set out the Board's good-faith estimate of the DAB Phase Financing Alt HAN Costs or, as applicable, Roll Out Financing Alt HAN Costs, that the Board anticipates will be incurred (or committed to) over whatever period the Board may determine provided such period shall be no longer than necessary to support the DAB Phase Financing or Roll Out Phase Financing, (as relevant);

(b) shall be accompanied by evidence showing the basis for any estimate provided in accordance with paragraph (a) above; and

(c) may make reasonable provision for contingencies.

Approval of Budgets

Z4.18 In relation to (1) the Draft Alt HAN Budget circulated in any Regulatory Year in respect of the next two Regulatory Years commencing thereafter and (2) any Draft Alt HAN Financing Budget, the Board shall:

(a) arrange for the circulation to all the Relevant Supplier Parties of the comments received from each Relevant Supplier Party regarding the Draft Alt HAN Budget or Draft Alt HAN Financing Budget during the 20 Working Days following the date of its circulation;

(b) consider and respond to those comments, and circulate its responses to all Relevant Supplier Parties;

(c) to the extent that it considers it appropriate to do so, amend the Draft Alt HAN Budget and/or the accompanying work plan or the Draft Alt HAN Financing Budget in the light of those comments; and

(d) submit that Draft Alt HAN Budget or Draft Alt HAN Financing Budget to the Forum for its approval, subject to any amendments that the Forum may determine,

and (1) the Draft Alt HAN Budget in such form as it may be approved by the Forum shall be the **Approved Alt HAN Budget** for the relevant Regulatory Year and (2) any Draft Alt HAN Financing Budget in such form as it may be approved by the Forum shall be an **Approved Alt HAN Financing Budget** for the period covered by any such Approved Alt HAN Financing Budget.

Z4.19 The Board shall, promptly upon its approval by the Forum, provide the DCC with a copy of the Approved Alt HAN Budget and any Approved Alt HAN Financing Budget, together (in each case) with such supporting information as may reasonably be requested by the DCC.

Amendments to Budgets

Z4.20 The Approved Alt HAN Budget relating to each Regulatory Year may be amended from time to time (whether before, during or after that Regulatory Year, and including in respect of Alt HAN Costs already incurred) and any Approved Alt HAN Financing Budget may be amended from time to time (including in respect of Alt HAN Costs already incurred), provided that, (in each case):

(a) the Board has first followed the procedure set out in Section Z4.18 in relation to the amendment as if it were a Draft Alt HAN Budget or a Draft Alt HAN Financing Budget; and

(b) the Forum has approved either the proposed amendment or such alternative amendment as it may determine.

Provision of Information to the DCC

Timetable

Z4.21 The Board shall take all reasonable steps to give effect to the provisions of Sections Z4.22 to Z4.29 so that a copy of each set of Approved Alt HAN Charging Data is provided to the DCC by no later than 1

December in the year prior to the commencement of the first Regulatory Year to which that Approved Alt HAN Charging Data relates.

Draft Alt HAN Charging Data

Z4.22 The Board shall during each Regulatory Year prepare and circulate to all Relevant Supplier Parties, the Secretary of State and the Authority draft information in respect of the Explicit Charges for Alt HAN Equipment for the next Regulatory Year commencing thereafter (the **Draft Alt HAN Charging Data**).

Z4.23 Each set of Draft Alt HAN Charging Data shall consist of the information:

(a) referred to in Section Z4.24 in respect of Central Shared Solution Alt HAN Equipment; and

(b) referred to in Section Z4.25 in respect of Central Point-to-Point Alt HAN Equipment.

Shared Solution Alt HAN Equipment

Z4.24 The information referred to in this Section Z4.24 is the Board's best estimate of:

(a) the total annual incremental cost of the provision of Alt HAN Services in the relevant Regulatory Year in respect of MPANs and MPRNs associated with premises in respect of which there is (or will be) installed Central Shared Solution Alt HAN Equipment;

(b) the average number of MPANs and MPRNs during the relevant Regulatory Year that will be associated with premises in respect of which there is (or will be) installed Central Shared Solution Alt HAN Equipment (excluding any in relation to which the Responsible Supplier has elected to use Opted-out Alt HAN Equipment); and

(c) the average monthly incremental cost (expressed in £ per Smart Metering System per month) of the provision of Alt HAN Services in the relevant Regulatory Year in relation to each MPAN and MPRN associated with premises in respect of which there is (or will be) installed Central Shared Solution Alt HAN Equipment during that Regulatory Year (excluding any in relation to which the Responsible Supplier has elected to use Opted-out Alt HAN Equipment).

Point-to-Point Alt HAN Equipment

Z4.25 The information referred to in this Section Z4.25 is the Board's best estimate of:

(a) the total annual incremental cost of the provision of Alt HAN Services in the relevant Regulatory Year in respect of Central Point-to-Point Alt HAN Equipment that will be (or will have been) provided to Parties by the end of the relevant Regulatory Year (whether provided during the relevant or previous Regulatory Year);

(b) the average number, during the relevant Regulatory Year, of items of Central Point-to-Point Alt HAN Equipment that will have been provided to Parties (whether provided in the relevant or any previous Regulatory Year);

(c) the average monthly incremental cost (expressed in £ per item of Central Point-to-Point Alt HAN Equipment) of the provision of Alt HAN Services in the relevant Regulatory Year in respect of Central Point-to-Point Alt HAN Equipment that will have been provided to Parties by the end of the Regulatory Year (whether provided during the relevant or any previous Regulatory Year); and

(d) the average monthly incremental cost (expressed in £ per MPAN and MPRN) of the provision of Alt HAN Services in the relevant Regulatory Year in relation to each MPAN and MPRN associated with premises in respect of which there is (or will be) installed Central Point-to-Point Alt HAN Equipment during that Regulatory Year (excluding any in relation to which the Responsible Supplier has elected to use Opted-out Alt HAN Equipment).

Z4.26 Not used.

Z4.27 The incremental costs referred to in Sections Z4.24 and Z4.25 shall include all the costs of making available and providing the relevant Alt HAN Services but shall not include any costs or expenses in relation to the carrying out of the Alt HAN Activities.

Approved Alt HAN Charging Data

Z4.28 In relation to the Draft Alt HAN Charging Data circulated in any Regulatory Year in respect of the next Regulatory Year commencing thereafter, the Board shall:

(a) arrange for the circulation to all the Relevant Supplier Parties of the comments received from each Relevant Supplier Party regarding the Draft Alt HAN Charging Data during the 20 Working Days following the date of its circulation;

(b) consider and respond to those comments, and circulate its responses to all Relevant Supplier Parties;

(c) to the extent that it considers it appropriate to do so (consistent with Section Z4.27) amend the Draft Alt HAN Charging Data; and

(d) submit that Draft Alt HAN Charging Data to the Forum for its approval, subject to any amendments that the Forum may (consistent with Section Z4.27) determine,

and the Draft Alt HAN Charging Data in such form as it may be approved by the Forum shall be the **Approved Alt HAN Charging Data** for the relevant Regulatory Year.

Z4.29 The Board shall, promptly upon its approval by the Forum, for the purposes of the determination by the DCC of Explicit Charges under Section K7.6(j), provide the DCC with a copy of the Approved Alt HAN Charging Data together with such supporting information as may reasonably be requested by the DCC.

The Alt HAN Inventory

Establishment and Maintenance of the Alt HAN Inventory

Z4.30 The Forum shall ensure that a database (the **Alt HAN Inventory**) is established and at all times maintained which shall include data in respect of:

(a) Central Shared Solution Alt HAN Equipment and Central Point-to-Point Alt HAN Equipment which has been installed in respect of premises, and the MPANs and MPRNs that are associated with those premises;

(b) Opted-out Alt HAN Equipment which has been installed at premises, and the MPANs and MPRNs associated with those premises; and

(c) where Opted-out Alt HAN Equipment has been installed in respect of premises, whether any Relevant Supplier Party which is the Responsible Supplier for a Smart Metering System that is capable of using that Opted-out Alt HAN Equipment has elected to use it in respect of an MPAN or MPRN with which it is associated.

Z4.31 Each Relevant Supplier Party shall ensure that the Alt HAN Inventory is promptly updated upon:

(a) the installation in respect of premises of Alt HAN Equipment which is capable of being used by a Smart Metering System in respect of which that Party is the Responsible Supplier;

(b) that Party electing either:

(i) to use any Opted-out Alt HAN Equipment which is capable of being used by a Smart Metering System in respect of which it is the Responsible Supplier; or

(ii) to cease to use any such Opted-out Alt HAN Equipment.

Z4.32 When a Relevant Supplier Party ensures that the Alt HAN Inventory is updated in accordance with Section Z4.31(a), it shall also ensure that the Alt HAN Inventory records whether the Alt HAN Equipment which has been installed is Opted-out Alt HAN Equipment or otherwise.

Z4.33 The information contained on the Alt HAN Inventory at any time shall be treated as conclusive evidence of whether a Relevant Supplier Party has elected at that time to use any Opted-out Alt HAN Equipment in respect of an MPAN or MPRN.

Z4.34 The Forum shall ensure that all Relevant Supplier Parties have available to them a means by which they can ensure that the Alt HAN Inventory is updated in accordance the requirements of Sections Z4.31 and Z4.32.

Provision of Information to the DCC

Z4.35 In each month of each year, the Board shall provide to the DCC the information set out in Section Z4.36, so that the information is:

(a) obtained by extracting it from the Alt HAN Inventory on the 15th day of that month; and

(b) provided to the DCC within five Working Days of being obtained.

Z4.36 The information set out in this Section Z4.36 is:

(a) for the purposes of the Explicit Charging Metric referred to at Section K7.5(t) ('shared solution Alt HAN Equipment'), a list of MPANs and MPRNs associated with premises in respect of which there is installed Central Shared Solution Alt HAN Equipment (excluding any MPAN or MPRN associated with premises in relation to which the Responsible Supplier has elected to use Opted-out Alt HAN Equipment);

(b) for the purposes of the Explicit Charging Metric referred to at Section K7.5(u) ('point-to-point solution Alt HAN Equipment'), a list of MPANs and MPRNs associated with premises in respect of which there is installed Central Point-to-Point Alt HAN Equipment to which the Alt HAN Services relate (excluding any MPAN or MPRN associated with premises in relation to which the Responsible Supplier has elected to use Opted-out Alt HAN Equipment); and

(c) for the purposes of the Explicit Charging Metric referred to at Section K7.5(v) ('stock level point-to-point solution Alt HAN Equipment'):

(i) a list of Parties which have been provided with Central Point-to-Point Alt HAN Equipment which has not yet been installed by or on behalf of a Relevant Supplier Party; and

(ii) a statement of the number of items of Central Point-to-Point Alt HAN Equipment which have been provided to each such Party and not yet installed by or on behalf of a Relevant Supplier Party.

Reports

Z4.37 The Board shall, as soon as is reasonably practicable following the end of each Regulatory Year, produce and circulate to:

(a) the Relevant Supplier Parties; and

(b) on request, the Secretary of State and the Authority,

a report on the Alt HAN Costs incurred (or committed to) during that Regulatory Year and the activities and projects to which those Alt HAN Costs relate.

Audit

Z4.38 The Board shall arrange for the monies paid by and to AltHANCo pursuant to this Section Z4 during each Regulatory Year to be audited by a firm of chartered accountants on an annual basis in order to verify whether the requirements of this Section Z4 have been met.

Z4.39 The Board shall send a copy of such auditor's report to all Relevant Supplier Parties and to the Authority within 10 Working Days of its receipt by the Board.

Z4.40 The Authority may from time to time require the Board to provide any information in relation to the Alt HAN Costs that the Authority may specify or describe in a notice given to the Board in accordance with this Section Z4.40, and the Board shall ensure that all such information is provided to the Authority by any date and in any format that the Authority may specify for that purpose.

Z4.41 The Authority may arrange for any such audit of the accounts and financial information of AltHANCo as it may consider appropriate for the purpose of verifying whether or not the Alt HAN Costs have been economically and efficiently incurred, and where it does so the Board shall co-operate fully with the Authority and any person acting on its behalf in order to ensure that any such audit is effective for that purpose.

Z5. TRANSITIONAL PROVISIONS

Forum Members

Z5.1 Where, prior to the coming into force of this Section Z, a Relevant Supplier Party:

(a) nominated a person to represent it in the Forum; and

(b) did not at a later date nominate any different person for that purpose in replacement for the person previously nominated, the person so nominated shall be treated as being a Forum Member on the date on which this Section Z comes into force.

Z5.2 For the purposes of this Section Z5, a person shall be treated as having been nominated by a Relevant Supplier Party if:

(a) that nomination was made in writing to the Secretary of State; and

(b) the nominating Party is a Relevant Supplier Party on the date on which this Section Z comes into force.

Forum Decisions

Z5.3 Where, prior to the coming into force of this Section Z, a decision was made:

(a) at a meeting of persons who were, at the date of that meeting, nominated by Relevant Supplier Parties to represent their interests in the Forum;

(b) in circumstances in which that meeting would be quorate if it took place on the day on which this Section Z comes into force;

(c) in relation to a matter on which a decision could be made by the Forum in accordance with this Section Z if it were made on the date on which this Section Z comes into force;

(d) in accordance with a process which could properly be followed by the Forum if it were followed on the date on which this Section Z comes into force;

(e) in a manner that is substantially consistent with the Forum Voting Protocol applicable on the date on which this Section Z comes into force;

(f) such that, if each person exercising a vote in respect of the relevant resolution at that meeting did so in the same way at a meeting taking place on the day on which this Section Z comes into force, the decision would be the same,

then that decision shall be treated as a decision of the Forum made on the date on which this Section Z comes into force, and for the purposes of this Section Z5 shall be referred to as a **Transitional Decision**.

Contrary Decisions

Z5.4 The making of a Transitional Decision shall not preclude the Forum from making any contrary decision on or after the date on which this Section Z comes into force, in which case the later decision shall prevail.

Forum Sub-Groups

Z5.5 By virtue of one or more Transitional Decisions, a Forum Sub-Group may be treated on the date on which this Section Z comes into force as being established and having duties, powers or functions delegated to it by the Forum, but no decision that was made by any Forum Sub-Group Members in any meeting prior to this Section Z coming into force shall be treated as having any binding effect.

Appeals

Z5.6 A Transitional Decision shall be capable of appeal, and the provisions of Sections Z1.61 to Z1.67 (Appeals from Decisions of the Forum) shall apply to it as they do to any other decision of the Forum.

Board Decisions

Z5.7 Where:

(a) prior to the coming into effect of this Section Z, any decision was made by the Board; and

(b) by virtue of paragraph 3 of the Annex to this Section Z, that decision has effect on and from the date on which this Section Z comes into effect,

that decision shall be capable of appeal, the provisions of Sections Z2.46 to Z2.48 (Appeals from Decisions of the Board) shall apply in relation to it as they do to any other decision of the Board, and for the purposes of those Sections the decision shall be treated as if it were made on the date on which this Section Z comes into effect.

Z6. DEFINITIONS

Z6.1 For the purpose of this Section Z, unless the context otherwise requires, the following words shall have the meaning given to them below:

Alt HAN Activities has the meaning given to that expression in Standard Condition 55.6 of the Electricity Supply Licence and Standard Condition 49.6 of the Gas Supply Licence

Alt HAN Costs has the meaning given to that expression in Section Z4.2 (Alt HAN Costs and Expenses).

Alt HAN Equipment has the meaning given to that expression in Standard Condition 55.8 of the Electricity Supply Licence and Standard Condition 49.8 of the Gas Supply Licence.

Alt HAN Inventory has the meaning given to that expression in Section Z4.30 (Establishment and Maintenance of the Alt HAN Inventory).

Alt HAN Secretariat has the meaning given to that expression in Section Z3.1 (Alt HAN Secretariat).

Alt HAN Services has the meaning given to that expression in Standard Condition 55.7 of the Electricity Supply Licence and Standard Condition 49.7 of the Gas Supply Licence.

Alternate Chair has the meaning given to that expression in Section Z1.10 (Election of Forum Chair and Alternate Chair).

AltHANCo has the meaning given to that expression in Section Z2.1 (Establishment of AltHANCo).

AltHANCo Election Protocol has the meaning given to that expression in Section Z2.14 (Election of Board Members).

AltHANCo Objectives has the meaning given to that expression in Section Z2.5 (AltHANCo Objectives).

Approved Alt HAN Budget has the meaning given to that expression in Section Z4.18 (Approval of Budgets).

Approved Alt HAN Charging Data has the meaning given to that expression in Section Z4.28 (Approved Alt HAN Charging Data).

Approved Alt HAN Financing Budget has the meaning given to that expression in Section Z4.18 (Approval of Budgets).

Board has the meaning given to that expression in Section Z2.3 (Establishment of AltHANCo).

Board Member has the meaning given to that expression in Section Z2.8 (Board Composition).

Central Point-to-Point Alt HAN Equipment means Point-to-Point Alt HAN Equipment which is not Opted-out Alt HAN Equipment.

Central Shared Solution Alt HAN Equipment means Shared Solution Alt HAN Equipment which is not Opted-out Alt HAN Equipment.

Chair has the meaning given to that expression in Section Z2.23 (Appointment of the Chair).

DAB Phase Financing means any debt financing entered into by AltHANCo for the purpose of financing Alt HAN Costs in respect of:

a. the design assurance and build phase of the technological solution development of the Alt HAN Equipment;
b. the operational mobilisation work necessary for the roll-out of the chosen Alt HAN Equipment; and
c. fees, costs and expenses in connection with the same.

DAB Phase Financing Alt HAN Costs has the meaning given that expression in Section Z4.2(c) (Alt HAN Costs and Expenses).

DCC Licence means the licence for the provision of a smart meter communication service granted pursuant to sections 6(1A) and (1C) of the Electricity Act 1989.

Draft Alt HAN Budget has the meaning given to that expression in Section Z4.15 (Draft Budgets and Work Plans).

Draft Alt HAN Charging Data has the meaning given to that expression in Section Z4.22 (Draft Alt HAN Charging Data).

Draft Alt HAN Financing Budget means a Draft Alt HAN (DAB Phase) Financing Budget, or a Draft Alt HAN (Roll Out) Financing Budget.

Draft Alt HAN (DAB Phase) Financing Budget has the meaning given to that expression in Section Z4.17A (Draft Budgets and Work Plans).

Draft Alt HAN (Roll Out) Financing Budget has the meaning given to that expression in Section Z4.17A (Draft Budgets and Work Plans).

Exempt Premises has the meaning given to that expression in Standard Condition 55.10 of the Electricity Supply Licence and Standard Condition 49.10 of the Gas Supply Licence.

Exempt Premises List has the meaning given to that expression in Standard Condition 55.12 of the Electricity Supply Licence and Standard Condition 49.12 of the Gas Supply Licence.

Explicit Charges has the meaning given to that expression in Section K11.1 (Definitions).

Explicit Charging Metrics has the meaning given to that expression in Section K11.1 (Definitions).

Forum Chair has the meaning given to that expression in Section Z1.10 (Election of Forum Chair and Alternate Chair).

Forum Member has the meaning given to that expression in Section Z1.7 (Appointment of Members).

Forum Objectives has the meaning given to that expression in Section Z1.3 (Forum Objectives).

Forum Sub-Group has the meaning given to that expression in Section Z1.42 (Establishing Forum Sub-Groups).

Forum Sub-Group Member has the meaning given to that expression in Section Z1.46 (Membership of Forum Sub-Groups).

Forum Voting Protocol means the SEC Subsidiary Document of that name set out in Appendix [TBC].

Opted-out Alt HAN Equipment means Alt HAN Equipment which is installed and maintained at premises otherwise than under and in accordance with the arrangements set out at this Section Z.

Relevant Preceding Period has the meaning given to that expression in Section Z1.30 (Voting).

Relevant Supplier Party means a Supplier Party which is required in accordance with standard condition 39 of an Electricity Supply Licence or standard condition 33 of a Gas Supply Licence (in each case entitled 'Smart Metering System – Roll-out, Installation and Maintenance') to install a Smart Metering System at any premises.

Roll Out Financing Alt HAN Costs has the meaning given that expression in Section Z4.2(d) (Alt HAN Costs and Expenses).

Roll Out Phase Financing means any debt financing entered into by AltHANCo for the purpose of raising finance to support the roll out of the Alt HAN Equipment, related ancillary services and any fees, costs and expenses in connection with the same.

Supplier Weighted Vote has the meaning given to that expression in Section Z1.27 (Voting).

Transitional Decision has the meaning given to that expression in Section Z5.3 (Forum Decisions).

SEC SCHEDULE 1 – FRAMEWORK AGREEMENT

Dated:________________2013

The Original Parties

and

Smart Energy Code Company Limited

Smart Energy Code Framework Agreement

THIS FRAMEWORK AGREEMENT is made on ______________2013

BETWEEN:

(1). the persons whose details are set out in the Schedule (the "Original Parties"); and

(2). **Smart Energy Code Company Limited** a company incorporated in England and Wales with company number 08430267 ("**SECCo**").

WHEREAS

(A). Certain of the Original Parties are the holders of Energy Licences that oblige them to be a party to, and to comply with, the Smart Energy Code.

(B). The Original Parties that do not hold an Energy Licence, or do not hold an Energy Licence that obliges them to be party to the Smart Energy Code, have chosen to become a party to the Smart Energy Code in order to receive Services from the DCC.

(C). SECCo is a company established to facilitate the operation of the Smart Energy Code.

(D). The Original Parties and SECCo have agreed to give effect to, and to be bound by, the Smart Energy Code in accordance with this Framework Agreement.

NOW IT IS HEREBY AGREED as follows:

1. Interpretation

1.1 In this Framework Agreement, including the recitals hereto, "Smart Energy Code" means the code of that name designated by the Secretary of State pursuant to the smart meter communication licences granted pursuant to the Electricity Act 1989 and the Gas Act 1986, as such code is modified from time to time in accordance with its provisions.

1.2 Subject to clause 1.1 above, the words and expressions used in this Framework Agreement shall be construed and interpreted in accordance with the definitions and provisions regarding interpretation set out in Section A (Definitions and Interpretation) of the Smart Energy Code, as if those definitions and provisions regarding interpretation were set out in this Framework Agreement and as if the references therein to "this Code" were to "this Framework Agreement".

2. Compliance with the Smart Energy Code

2.1 With effect from the date hereof, SECCo and each of the Original Parties hereby undertakes, for the benefit of each other Party from time to time, to comply with the Smart Energy Code in accordance with, and subject to, its terms and conditions.

3. Identity of the Parties

3.1 SECCo and each of the Original Parties acknowledges that it has agreed a mechanism (set out in Section B

(Accession) of the Smart Energy Code) by which New Parties may become bound by the Smart Energy Code, each of whom will then become a Party for the purposes of clause 2 above (and otherwise).

3.2 Each of the Original Parties acknowledges that it has agreed a mechanism (set out in Section M8 (Suspension, Expulsion and Withdrawal) of the Smart Energy Code) by which it may cease to be bound by the Smart Energy Code, from which time it will (subject to Section M8 of the Smart Energy Code) cease to be obliged to comply with the Smart Energy Code.

3.3 SECCo and each of the Original Parties acknowledges that it has agreed a mechanism (set out in Section M8 (Suspension, Expulsion and Withdrawal) of the Smart Energy Code) by which other Parties may cease to be bound by the Smart Energy Code, from which time such other Parties will (subject to Section M8 of the Smart Energy Code) cease to be a Party for the purposes of clause 2 above (and otherwise).

4. Party Details

4.1 The Party Details for each of the Original Parties shall (as at the date hereof, and subject to future amendment in accordance with Section M6 (Party Details) of the Smart Energy Code) be those details set out as such in the Schedule.

5. Third Party Rights

5.1 Without prejudice to any provisions of the Smart Energy Code permitting enforcement of the Smart Energy Code by third parties, the Original Parties do not intend that any of the terms or conditions of this Framework Agreement will be enforceable by a third party (whether by virtue of the Contracts (Rights of Third Parties) Act 1999 or otherwise).

6. Counterparts

6.1 This Framework Agreement may be executed in any number of counterparts, each of which shall be an original but all of which together shall constitute one and the same instrument. The counterpart executed by each of the Original Parties shall attach a schedule containing details of the relevant Original Party, all of which schedules together shall comprise the "Schedule".

7. Governing Law and Jurisdiction

7.1 This Framework Agreement and any dispute or claim arising out of or in connection with it (including non-contractual claims) shall be governed by, and construed in accordance with, the laws specified in Section M11 (Miscellaneous) of the Smart Energy Code from time to time for the purpose of disputes or claims arising out of or in connection with the Smart Energy Code.

7.2 In relation to any dispute or claim arising out of or in connection with this Framework Agreement (including in respect of non-contractual claims), each of the Original Parties and SECCo irrevocably agrees to submit to the exclusive jurisdiction of the relevant person, panel, court or other tribunal specified in Section M7 (Dispute Resolution) of the Smart Energy Code from time to time for the purpose of disputes or claims of that nature.

THIS FRAMEWORK AGREEMENT has been executed and delivered as a **DEED** on the date first stated above.

Executed and delivered as a deed by

…………………………………………

Print full name of Original Party …………………………………………

acting by an attorney appointed under a power of attorney

Print name of attorney

Signature ………………………………………….

In the presence of:

…………………………………………
Print name of witness

Signature ………………………………………….

Address ………………………………………….

OR

Executed and delivered as a deed by

…………………………………………
Print name of person signing

…………………………………
Print full name of Original Party

acting by two directors or a director and the company secretary

Signature ………………………………………….

…………………………………………
Print name of person signing

Signature ………………………………………….

Schedule to the Framework Agreement – Original Parties

(1). The Party's full name.

(2). Whether the Party is a company or a natural person or a partnership etc.

(3). The Party's jurisdiction of incorporation (if applicable).

(4). The Party's registered number (if applicable).

(5). The Party's registered address (or, if not applicable, its principal address).

(6). Where the Party is incorporated or resident outside Great Britain, an address in Great Britain for the receipt of legal notices on the Party's behalf.

(7). The Party's VAT registration number (if applicable).

(8). The Party's address for invoices under the Code.

(9). The Party's address or addresses for all other notices under the Code.

(10). The Party Category into which the Party considers it will initially fall.

(11). The Energy Licences held by the Party (including any for which it has applied).

(12). Details of any Parties that are Affiliates of the Party (where the Party is a company).

(13). Where the Party holds one or more Energy Licences, details of any unique identifiers by which the Party is identified under the MRA and/or the UNC (as applicable).

SEC SCHEDULE 2 – ACCESSION AGREEMENT

Dated:2[XXX]

[New Party]

and

Smart Energy Code Company Limited

Smart Energy Code
Accession Agreement

THIS ACCESSION AGREEMENT is made on2[XXX]

BETWEEN:

(1). [**TBC**] a company incorporated in [Jurisdiction] (registered number [TBC]) whose registered office is at [TBC] (the "**New Party**"); and

(2). **Smart Energy Code Company Limited** a company incorporated in England and Wales with company number 08430267 ("**SECCo**").

WHEREAS

(A). The New Party is either obliged by its Energy Licence to become a party to the Smart Energy Code, or wishes to become a party to the Smart Energy Code in order to receive Services from the DCC.

(B). SECCo is authorised by the Parties to the Smart Energy Code to accept the accession to the Smart Energy Code of the New Party.

NOW IT IS HEREBY AGREED as follows:

1. Interpretation

1.1 In this Accession Agreement, including the recitals hereto, "**Smart Energy Code**" means the code of that name designated by the Secretary of State pursuant to the smart meter communication licences granted pursuant to the Electricity Act 1989 and the Gas Act 1986, as such code is modified from time to time in accordance with its provisions.

1.2 Subject to clause 1.1 above, the words and expressions used in this Accession Agreement shall be construed and interpreted in accordance with the definitions and provisions regarding interpretation set out in Section A (Definitions and Interpretation) of the Smart Energy Code, as if those definitions and provisions regarding interpretation were set out in this Accession Agreement and as if the references therein to "this Code" were to "this Accession Agreement".

2. Compliance with the Smart Energy Code

2.1 With effect from the date hereof, the New Party hereby undertakes, for the benefit of SECCo and each other Party from time to time, to comply with the Smart Energy Code in accordance with, and subject to, its terms and conditions.

3. Identity of the Parties

3.1 The New Party acknowledges that the Original Parties became bound by the Smart Energy Code pursuant to the Framework Agreement, and that each such Original Party is a Party for the purposes of clause 2 above (and otherwise).

3.2 The New Party acknowledges that it has agreed a mechanism (set out in Section B (Accession) of the Smart Energy Code) by which New Parties other than itself may have (or may in the future) become bound by the

Smart Energy Code, each of whom is (or will then become) a Party for the purposes of clause 2 above (and otherwise).

3.3 The New Party acknowledges that it has agreed a mechanism (set out in Section M8 (Suspension, Expulsion and Withdrawal) of the Smart Energy Code) by which it may cease to be bound by the Smart Energy Code, from which time it will (subject to Section M8 of the Smart Energy Code) cease to be obliged to comply with the Smart Energy Code.

3.4 The New Party acknowledges that it has agreed a mechanism (set out in Section M8 (Suspension, Expulsion and Withdrawal) of the Smart Energy Code) by which other Parties may cease to be bound by the Smart Energy Code, from which time such other Parties will (subject to Section M8 of the Smart Energy Code) cease to be a Party for the purposes of clause 2 above (and otherwise).

4. Party Details

4.1 The New Party's Party Details shall (as at the date hereof, and subject to future amendment in accordance with Section M6 (Party Details) of the Smart Energy Code) be those details set out as such in the Schedule.

5. Third Party Rights

5.1 Without prejudice to any provisions of the Smart Energy Code permitting enforcement of the Smart Energy Code by third parties, neither the New Party nor

5.2 SECCo intends that any of the terms or conditions of this Accession Agreement will be enforceable by a third party (whether by virtue of the Contracts (Rights of Third Parties) Act 1999 or otherwise).

6. Execution

6.1 This Accession Agreement may be executed in any number of counterparts, each of which shall be an original but all of which together shall constitute one and the same instrument.

6.2 Where the Code Administrator has provided unexecuted counterparts of this Accession Agreement to the New Party, the New Party should sign (but not date) both counterparts of this Accession Agreement, and return them to the Code Administrator. In doing so, the New Party will be deemed to have authorised SECCo (by its signature of the counterparts) to complete the agreement and to date the counterparts with the date of such completion.

7. Governing Law and Jurisdiction

7.1 This Accession Agreement and any dispute or claim arising out of or in connection with it (including non-contractual claims) shall be governed by, and construed in accordance with, the laws specified in Section M11 (Miscellaneous) of the Smart Energy Code from time to time for the purpose of disputes or claims arising out of or in connection with the Smart Energy Code.

7.2 In relation to any dispute or claim arising out of or in connection with this Accession Agreement (including in respect of non-contractual claims), each of the New Party and SECCo irrevocably agrees to submit to the exclusive jurisdiction of the relevant person, panel, court or other tribunal specified in Section M7 (Dispute Resolution) of the Smart Energy Code from time to time for the purpose of disputes or claims of that nature.

THIS ACCESSION AGREEMENT has been executed and delivered as a **DEED** on the date first stated above.

Executed and delivered as a deed by …………………………………………
Print name of person signing

…………………………………
Print full name of New Party

acting by two directors or a director and the company secretary

Signature …………………………………………

…………………………………………
Print name of person signing

Signature …………………………………………

Executed and delivered as a deed by …………………………………………

…………………………………………
Print name of person signing

Smart Energy Code Company Limited

Signature …………………………………………

acting by two directors or a director and the company secretary

…………………………………………
Print name of person signing

Signature …………………………………………

Schedule to the Accession Agreement – Party Details

[To include the information referred to in paragraphs 6 to 15 (inclusive) of Schedule 5 (Accession Information).]

SEC SCHEDULE 3 – SPECIMEN BILATERAL AGREEMENT

Dated:2[XXX]

[User]

and

[DCC]

Smart Energy Code
Bilateral Agreement

THIS BILATERAL AGREEMENT is made on 2[XXX]

BETWEEN:

(1). [**TBC**] a company incorporated in [Jurisdiction] (registered number [TBC]) whose registered office is at [TBC] (the "**User**"); and

(2). [**TBC**] a company incorporated in [Jurisdiction] (registered number [TBC]) whose registered office is at [TBC] (the "**DCC**").

WHEREAS

(A). The User wishes to procure the Elective Communication Service pursuant to the Smart Energy Code.

(B). The DCC has agreed to provide the Elective Communication Service pursuant to this Bilateral Agreement and the Smart Energy Code, in consideration of the Elective Charges.

NOW IT IS HEREBY AGREED as follows:

1. Interpretation

1.1 In this Bilateral Agreement, unless the context otherwise requires:

"**Elective Charges**" means the charges described as such in Schedule 1.

"**Elective Communication Service**" means the service described as such in Schedule 2.

"**Smart Energy Code**" means the code of that name designated by the Secretary of State pursuant to the smart meter communication licences granted to the DCC pursuant to the Electricity Act 1989 and the Gas Act 1986, as such code is modified from time to time in accordance with its provisions.

1.2 In this Bilateral Agreement, unless the context otherwise requires, references to "Clauses" and "Schedules" are to the clauses of, and schedules to, this Bilateral Agreement.

1.3 Subject to Clauses 1.1 and 1.2, the words and expressions used in this Bilateral Agreement shall be construed and interpreted in accordance with the definitions and provisions regarding interpretation set out in Section A (Definitions and Interpretation) of the Smart Energy Code, as if those definitions and provisions regarding interpretation were set out in this Bilateral Agreement and as if the references therein to "this Code" were to "this Bilateral Agreement".

1.4 The Parties acknowledge that the Smart Energy Code is subject to modification from time to time in accordance with its provisions, and that the Smart Energy Code as so modified from time to time shall apply for the purposes of this Bilateral Agreement. References to Sections of the Smart Energy Code shall be to those sections as modified and/or renumbered from time to time.

1.5 The provisions of this Bilateral Agreement are without prejudice to the rights and obligations of the Parties under the Smart Energy Code. The Parties acknowledge that certain provisions of the Smart Energy Code apply, but such acknowledgments are without prejudice to the potentially broader application of the Smart Energy Code. In the event of any conflict between the provisions of this Bilateral Agreement and the provisions of the Smart Energy Code, the Smart Energy Code shall prevail.

2. Commencement of this Bilateral Agreement

2.1 This Bilateral Agreement shall commence on [TBC][1].

3. Provision of the Elective Communication Services

3.1 The DCC shall provide the Elective Communication Services to the User subject to and in accordance with this Bilateral Agreement and the Smart Energy Code.

3.2 The provision of the Elective Communication Services is subject to the User having completed the User Entry Process. The provision of the Elective Communication Services in respect of any Smart Metering System is subject to that Smart Metering System having been Enrolled.

4. Elective Charges

4.1 The User shall pay the Elective Charges in accordance with Section J (Charges) of the Smart Energy Code.

4.2 [The Elective Charges include a standing charge (as further described in Schedule 1) that is payable by the User regardless of whether or not the Elective Communication Services are requested or provided.][2]

5. Security and Data Privacy

5.1 The Parties acknowledge that the provisions of Section G (Security) of the Smart Energy Code apply.

5.2 The Parties acknowledge that the provisions of Section I (Data Privacy) of the Smart Energy Code apply.

6. Termination or Expiry of this Bilateral Agreement

6.1 Subject to earlier termination in accordance with this Clause 6, this Bilateral Agreement shall expire on [TBC].

6.2 This Bilateral Agreement shall automatically terminate on the User being expelled from, or voluntarily ceasing to be party to, the Smart Energy Code in accordance with Section M8 (Suspension, Expulsion and Withdrawal) of the Smart Energy Code.

6.3 The User shall, at its discretion, be entitled to terminate this Bilateral Agreement on 20 Working Days' prior notice in writing to the DCC.

[1] [*Note: consider whether agreement should be conditional on provision of adequate credit support. If so, also add a termination right linked to failure of credit support.*]

[2] [*Note: delete or retain as applicable.*]

6.4 In the event of termination of this Bilateral Agreement in accordance with Clause 6.3, the User shall not be obliged to pay compensation on termination to the extent such compensation is intended to recover investments made for the purposes of providing the Elective Communication Service where (and to the extent that)the DCC subsequently offers a Service listed in the DCC User Interface Services Schedule that relies upon such investments. Any dispute under this Clause 6.4 may be referred to the Panel for initial determination, but shall ultimately be subject to arbitration.

6.5 Where this Bilateral Agreement terminates in accordance with Clause 6.2 or 6.3, the User shall (subject to Clause 6.4) pay any compensation on termination described in Schedule 1.

7. Suspension

7.1 The User acknowledges that the DCC may suspend provision of the Elective Communication Services where the Panel directs that the DCC should do so pursuant to Section M8 (Suspension, Expulsion and Withdrawal) of the Smart Energy Code. Such suspension shall be without prejudice to any take or pay obligation described in Schedule 1.

8. Communications

8.1 The Parties acknowledge and agree that the provisions of Sections H3 (DCC User Gateway) and M10 (Notices) apply.

9. Amendments

9.1 Without prejudice to Clause 1.4, this Bilateral Agreement may only be amended by agreement in writing by the Parties or in order to give effect to any determination of disputes by the Authority pursuant to the DCC Licence.

9.2 Without prejudice to Clause1.5, the Parties shall amend this Bilateral Agreement where it has become inconsistent with the Smart Energy Code in order to correct such inconsistency (including where the Specimen Bilateral Agreement is modified, in which case the Parties shall amend this Bilateral Agreement in the same manner and to the same extent).

9.3 The User hereby authorises the DCC to make the amendments to this Bilateral Agreement required pursuant to Clause 9.2 on the User's behalf. Where the User disputes the requirement for, or form of, any such amendments made by the DCC on the User's behalf, then the User may refer the matter to the Panel for its determination. Nothing in this Clause 9.3 shall fetter the User's right to refer disputes to the Authority pursuant to the DCC Licence.

10. Miscellaneous

10.1 The Parties acknowledge that the provisions of Sections M2 (Limitations of Liability), M3 (Services FM and Force Majeure), M4 (Confidentiality), and M5 (Intellectual Property Rights) of the Smart Energy Code apply.

10.2 The Parties acknowledge and agree that this Bilateral Agreement may be novated to DCC's successor in accordance with Section M9 (DCC Transfer) of the Smart Energy Code.

10.3 This Bilateral Agreement may be executed in any number of counterparts, each of which shall be an original but all of which together shall constitute one and the same instrument.

10.4 The provisions of Section M11 (Miscellaneous) of the Smart Energy Code shall apply as if set out in this Bilateral Agreement and as if the references therein to "this Code" were to "this Bilateral Agreement".

11. Governing Law and Jurisdiction

11.1 This Bilateral Agreement and any dispute or claim arising out of or in connection with it (including non-contractual claims) shall be governed by, and construed in accordance with, the relevant laws specified in Section M11 (Miscellaneous) of the Smart Energy Code from time to time for the purpose of disputes or claims of that nature.

11.2 In relation to any dispute or claim arising out of or in connection with this Bilateral Agreement (including in respect of non-contractual claims), each of the Parties irrevocably agrees to submit to the exclusive jurisdiction of the relevant person, panel, court or other tribunal specified in Section M7 (Dispute Resolution) of the Smart Energy Code from time to time for the purpose of disputes or claims of that nature.

THIS BILATERAL AGREEMENT has been entered into on the date first stated above.

SIGNED by

duly authorised for and on behalf of …………………………………………

Print name of person signing

…………………………………………

Print full name of User

Signature

………………………………………….

SIGNED by

duly authorised for and on behalf of the DCC …………………………………………

Print name of person signing

Signature

………………………………………….

Schedule 1 – Elective Charges

[Note: to include charges determined in accordance with the Charging Methodology, and to include standing charges and early termination compensation payments where required in accordance with Section H7.]

Schedule 2 – Elective Communication Services

[Note: to identify services in a manner consistent with the DCC User Interface Services Schedule and Section H7.14.]

SEC SCHEDULE 4 – SECCO

1. Background

1.1 Smart Energy Code Company Limited (registered in England and Wales with company number 08430267) ("SECCo") has been established on behalf of the Parties in order to fulfil the Objective (as defined below), and in doing so will act as the contracting body for the Panel.

1.2 It is intended that the shareholders of SECCo shall be limited to Eligible Parties in accordance with this Schedule.

1.3 The Shareholders have agreed that their respective rights as Shareholders shall be regulated by the provisions of this Schedule. The rights of the Eligible Parties as Shareholders are set out exclusively in this Schedule. No other provision of this Code shall apply to the regulation of the rights and obligations of Shareholders in their capacity as Shareholders.

1.4 SECCo has agreed with the Shareholders to comply with the provisions of this Schedule insofar as it relates to SECCo.

2. Additional Definitions and Interpretation

2.1 In this Schedule, except where the context otherwise requires, the following words and expressions shall have the following meanings:

Articles means the articles of association of SECCo, as amended from time to time.

Board means the board of directors of SECCo at the relevant time.

Director means a director of SECCo from time to time.

Eligible Party means a Party that is not the DCC (which, for the avoidance of doubt, does not include SECCo), and which either:

(a) holds an Energy Licence that obliges it to be a party to this Code; or

(b) does not hold an Energy Licence that obliges it to be a party to this Code, but has opted (by notice in writing to the SECCo Secretary) to be a Shareholder.

Objective means acting as a corporate vehicle to assist the Panel in exercising its powers, duties and functions (including entering into contracts where necessary or desirable in order to implement any Panel Decision).

Panel Decision means a resolution of the Panel (or a resolution made by any Sub-Committee to which the Panel has delegated decision-making authority in accordance with Section C7 (Sub-Committees)), and cognate terms shall be construed accordingly.

Retiring Shareholder means either:

(c) a Shareholder that ceases to be a Party; or

(d) a Shareholder that does not hold an Energy Licence that obliges it to be a party to this Code and which gives notice that it no longer wishes to be a Shareholder (such notice to be given in writing to the SECCo Secretary).

SECCo Chair means the chairman of the Board from time to time.

SECCo Secretary means the company secretary of SECCo from time to time.

Share means an ordinary share of £1 each in the share capital of SECCo.

Shareholder means a person from time to time registered as a holder of a Share.

Subscribing Shareholders means each Eligible Party that agreed (prior to the designation of this Code) to become a Shareholder with effect from the designation of this Code.

2.2 Words and expressions defined elsewhere in this Code shall have the same meaning in this Schedule unless the context otherwise requires.

3. Acknowledgement of Preliminary Matters Already Undertaken

3.1 It is acknowledged that resolutions of the Board and of the Shareholders were made prior to the designation of this Code, at which the business set out in annex 1 to this Schedule was undertaken. As set out in that annex, such business is to have effect from the designation of this Code.

3.2 The consequence of the resolutions referred to above is that, with effect from the designation of this Code, each of the Subscribing Shareholders is a Shareholder and each of the Panel Members is a Director.

4. SECCo's Objective

4.1 The Shareholders and SECCo acknowledge and agree that SECCo shall not undertake any activities other than those that are reasonably necessary for carrying out the Objective.

4.2 Each Shareholder acknowledges and agrees that SECCo will have complete independence from its Shareholders in its operations and undertakes not to take any action which obstructs or interferes with, or seeks to obstruct or interfere with, the carrying out of the Objective (provided that this Paragraph 4.2 shall not restrict the exercise of Shareholder rights in order to comply with the requirements of this Schedule).

5. SECCo's Business

5.1 Each Shareholder agrees with each other Shareholder to exercise its rights under this Schedule and as a Shareholder in SECCo so as to ensure that:

(a) SECCo performs and complies with all its obligations under this Code (including without limitation this Schedule) and complies with the restrictions (if any) imposed on it by the Articles; and

(b) SECCo's activities are conducted in accordance with sound and good business practice with a view to achieving the Objective.

6. New Shareholders

6.1 Any Eligible Party, from time to time, which is not a Shareholder may apply to the SECCo Secretary to become a Shareholder. An Eligible Party holding an Energy Licence that obliges it to be a party to this Code shall be deemed to have so applied on its accession to this Code pursuant to Section B (Accession). Upon any such application, the Directors shall either:

(a) procure the transfer to such Eligible Party of one Share then held by a nominee in accordance with Paragraph 7.2 or 7.3; or

(b) allot to such Eligible Party one Share.

6.2 For the purposes of Paragraph 6.1(b), the Shareholders agree that, where no Shares are otherwise available for issue, they will exercise the voting rights attaching to their Shares to procure that all necessary steps are taken to create and/or authorise the issue of further Shares.

7. Dealings with Shares

7.1 Otherwise than in accordance with the following provisions of this Paragraph 7, no Shareholder shall:

(a) pledge, mortgage (whether by way of fixed or floating charge) or otherwise encumber its legal or beneficial interest in its Shares; or

(b) sell, transfer or otherwise dispose of any of such Shares (or any legal or beneficial interest therein); or

(c) enter into any agreement in respect of the votes attached to Shares; or

(d) agree, whether or not subject to any condition precedent or subsequent, to do any of the foregoing.

7.2 Upon written notice by the Board requiring it to do so, a Retiring Shareholder shall pay up all amounts which remain unpaid on any Share held by it. The Retiring Shareholder will transfer its Shares at par to a nominee who will hold the Shares for and on behalf of all the other Shareholders. The nominee will be selected by the Directors. All costs and expenses of such transfer shall be for the account of the Retiring Shareholder.

7.3 If a Retiring Shareholder fails or refuses to transfer any Shares in accordance with its obligations under Paragraph 7.2, the Retiring Shareholder irrevocably appoints by way of security for the failure to perform obligations under this Paragraph 7.3 any Director to execute and deliver a transfer of the Shares from the Retiring Shareholder to a nominee on behalf of the Retiring Shareholder. SECCo may accept the consideration for the transfer (subject to the Retiring Shareholder paying-up all amounts which remain unpaid on any Share) and hold it on trust for the Retiring Shareholder, which acceptance shall be a good discharge to the nominee, and may set off such amounts against the costs and expenses of the transfer. The Directors shall cause the nominee to be registered as the holder of such Share and, following the registration of the transfer, the validity of the proceedings shall not be questioned by SECCo or any Shareholder.

7.4 The nominee referred to in Paragraphs 7.2 and 7.3 shall hold Shares transferred to it until such time as it is directed by the Directors to transfer them (or some of them) in accordance with Paragraph 6.1(a) and for such period (and only for such period) as the nominee holds any Shares, all rights attaching to the Share shall be suspended, including:

(a) the right to receive income and/or capital;

(b) the right to attend and vote or appoint proxies to attend and vote at general meetings of SECCo (whether on a show of hands or on a poll and in the case of proxies only on a poll); and

(c) the right to appoint and remove a Director.

7.5 The Shareholders shall procure that, save in the case of any nominee for the purposes of Paragraphs 7.2 and 7.3:

(a) no person who is not an Eligible Party may at any time become a Shareholder; and

(b) no Eligible Party shall hold more than one Share at any time,

and the Directors shall be entitled to refuse to allot and/or to register any transfer of a Share that would result in a breach of this Paragraph 7.5.

8. Composition and Proceedings of the Board

8.1 SECCo and the Shareholders acknowledge that this Code contains detailed provisions regarding the composition of the Panel, and that it is the intention of SECCo and the Shareholders that the composition of the Board is identical to the composition of the Panel. The Shareholders shall, accordingly, procure that:

(a) each of the Panel Members from time to time shall be appointed as a Director; and

(b) the Panel Chair from time to time shall be appointed as the SECCo Chair.

8.2 SECCo and the Shareholders acknowledge that this Code contains detailed provisions regarding the procedural rules of the Panel, and that it is the intention of SECCo and the Shareholders that the procedural rules of the Board are identical to the procedural rules of the Panel. The remaining provisions of this Paragraph 8 shall therefore have effect subject to the procedural rules of the Board set out in Section C (Governance); save only to the extent that such procedural rules applicable to the Panel are incompatible with Laws and Directives stipulating procedural rules for company boards of directors.

8.3 Each Director shall be deemed to have appointed his or her Alternate as his or her alternate Director, and shall be deemed to have removed such person from such position on that person ceasing to be his or her Alternate. Any such alternate Director shall be entitled to receive notice of all Board meetings and attend and vote as such at any meeting at which the appointing Director is not present and generally in the absence of his or her appointor to do all the things which his or her appointor is authorised or empowered to do. A Director who is also an alternate is entitled, in the absence of his or her appointor:

(a) to a separate vote on behalf of his or her appointor in addition to his or her own vote; and

(b) to be counted as part of the quorum of the Board on his or her own account and also in respect of the Director for whom he or she is the alternate.

8.4 If a Director ceases to be a Panel Member, the Shareholders shall exercise their powers to ensure that such person ceases to be a Director. The DCC shall indemnify SECCo against all Liabilities which SECCo may suffer or incur by reason of any claim by that person in connection with his removal from office as a Director.

8.5 The SECCo Chair shall chair any Board meeting. If the SECCo Chair is unable to be present at a Board meeting, the SECCo Chair's alternate appointed in accordance with Paragraph 8.3 may act as chair of that Board meeting.

8.6 The person appointed from time to time as the Secretariat shall be appointed as the SECCo Secretary.

8.7 All resolutions of the Board shall be made by simple majority of those Directors present at the meeting. Each Director shall have one vote, provided that the SECCo Chair shall have no vote (except in the case of equality of votes, in which case the SECCo Chair shall have the casting vote). Notwithstanding the foregoing, in the case of the person appointed as SECCo Chair by virtue of being Panel Chair in accordance with Section X (Transition), that person shall have a vote as a Director and shall not have any casting vote.

8.8 The Board shall meet at intervals of not less than once in any period of two months unless otherwise agreed by the Directors. Insofar as reasonably practicable, meetings of the Board shall follow on immediately from meetings of the Panel. A meeting of the Board may be convened at any reasonable time at the request of any Director by written notice to the SECCo Secretary.

8.9 Meetings of the Board may be held by means of any telecommunications equipment provided that each of the Directors attending the meeting acknowledges that he or she can communicate with each other. In any such case, the meeting shall be deemed to take place in the location of the SECCo Chair during such meeting.

8.10 Each of the Directors shall be given notice by the SECCo Secretary of each meeting of the Board setting out details of the time, date and place of meeting at least 10 Working Days prior to the date of such meeting (provided that such period of notice may be shortened for particular meetings by unanimous written consent of all Directors entitled to attend and vote at the meeting).

8.11 The quorum for each meeting of the Board is one half of all Directors appointed at the relevant time, at least one of whom must be the SECCo Chair (or his or her alternate as such).

8.12 A written resolution signed by a majority of the Directors shall be as valid and effective as a resolution passed by a meeting of the Board properly convened and constituted in accordance with the terms of this Schedule and the Articles.

8.13 As soon as reasonably practicable and in any event no later than five Working Days after each Board meeting, the SECCo Secretary shall circulate minutes of that meeting to each of the Directors.

8.14 The Board may delegate any of its powers to committees of the Board consisting of such persons as the Board may resolve. Any such committee shall exercise only powers expressly delegated to it and shall comply with any regulations imposed on it by the Board.

9. Expenditure and Working Capital

9.1 The Shareholders intend that SECCo should be run on a “break even” basis and shall procure that any surplus working capital shall, rather than being distributed to Shareholders, be retained by SECCo and applied to subsequent expenditure.

9.2 None of the Shareholders shall be obliged to provide any finance to SECCo or to provide any guarantee, indemnity or other security which third parties may require to secure the obligations of SECCo.

9.3 The Shareholders shall exercise the rights attaching to their Shares with a view to ensuring that SECCo does not incur costs unless authorised to do so in accordance with Section C8 (Panel Costs and Budgets), except insofar as is necessary in order to comply with legally binding obligations to which SECCo is subject.

10. Accounts

10.1 As soon as reasonably practicable following the end of each Regulatory Year, SECCo shall procure that an account shall be taken of all the assets and liabilities of SECCo and of all the dealings and transactions of SECCo during such Regulatory Year.

10.2 The Board shall prepare a report and accounts in accordance with the Companies Act 2006 to be audited within three months after the end of each Regulatory Year.

11. Conflict with the Articles

11.1 In the event of any ambiguity created by or discrepancy between the provisions of this Schedule and the Articles, it is the intention that the provisions of this Schedule shall prevail and accordingly the Shareholders shall exercise all voting and other rights and powers available to them so as to give effect to the provisions of this Schedule and shall further, if necessary, procure any required amendment to the Articles.

11.2 Any Shareholder failing to comply with the provisions of Paragraph 11.1 shall be deemed to have appointed SECCo as its lawful attorney for the purpose of signing any written resolution (or receiving notices of and attending and voting at all meetings) of the members of the SECCo to give effect to the provisions of Paragraph 11.1 and to effect any required amendment to the Articles (including to conform the Articles to this Schedule), and this power of attorney (which is given by way of security to secure the performance of obligations owed by the Shareholder to the SECCo under Paragraph 11.1) shall be irrevocable.

12. Further Assurance

Each Shareholder shall co-operate with the other Shareholders and execute and deliver to the other Shareholders such other instruments and documents and take such other actions as may be reasonably requested from time to time in order to carry out, evidence and confirm their rights under, and the intended purpose of, this Schedule.

13. Duration and Termination

13.1 This Schedule shall continue in full force and effect, save in respect of any antecedent breach, until the earlier of:

(a) the termination of this Code; and

(b) the date on which an effective resolution is passed, or a binding order is made, for the winding up of SECCo, provided, however, that this Schedule shall cease to have effect as regards any Eligible Party who, having been entitled under the terms of this Schedule to hold Shares, ceases to hold any Shares.

provided, however, that this Schedule shall cease to have effect as regards any Eligible Party who, having been entitled under the terms of this Schedule to hold Shares, ceases to hold any Shares.

ANNEX 1

Prior to designation of this Code, SECCo (acting by its directors from time to time) and/or the shareholders of SECCo (as applicable) approved the following matters:

1. the change of name of SECCo to Smart Energy Code Company Limited;

2. the transfer of the subscription share in the capital of SECCo to a nominee as if Paragraph 7.2 applied;

3. the change of the registered office of SECCo to the registered address of the Secretariat;

4. the change of the accounting reference date of SECCo to 31 March;

5. the adoption of new Articles of Association of SECCo as per Annex 2;

6. the subscription for Shares in SECCo by the Subscribing Shareholders;

7. the appointment as Directors of SECCo of the Panel Members nominated pursuant to Section X (Transition);

8. the appointment as the company secretary of SECCo of the Secretariat nominated pursuant to Section X (Transition);

9. conflicts of interest (if any) of the incoming Directors of SECCo;

10. the resignation of the incumbent Director of SECCo appointed at incorporation; and

11. the filings at Companies House and updates to the statutory books of SECCo in relation to the matters referred to at 1 – 10 above.

ANNEX 2

Form of New Articles

ARTICLES OF ASSOCIATION

THE COMPANIES ACT 2006

ARTICLES OF ASSOCIATION

of

Smart Energy Code Company Limited (the "Company")

(Registered No. 08430267)

(adopted by Special Resolution passed on [ ])

1. Defined terms

1.1 In these articles:

"**CA 2006**" means the Companies Act 2006;

"**Code**" means the Smart Energy Code designated by the Secretary of State pursuant to the smart meter communication licences granted pursuant to the Electricity Act 1989 and the Gas Act 1986, as such code is modified from time to time in accordance with its provisions;

"**Companies Acts**" means the Companies Acts (as defined in section 2 of the CA 2006), in so far as they apply to the company;

"**connected persons**" in relation to a director means persons connected with that director for the purposes of section 252 CA 2006;

"**eligible director**" means, in relation to a matter or decision, a director who is or would be entitled to count in the quorum and vote on the matter or decision at a meeting of directors (but excluding any director whose vote is not to be counted in respect of the particular matter or decision);

"**Group Company**" means a body corporate which is at the relevant time:

(a) a subsidiary of the Company; or

(b) the Company's holding company or a subsidiary of that holding company,

and for these purposes "**holding company**" and "**subsidiary**" have the meanings given to those expressions in section 1159 CA 2006;

"**Model Articles**" means the regulations contained in Schedule 3 to The Companies (Model Articles) Regulations 2008; and

"**Panel**" has the meaning given to that expression in the Code.

1.2 Unless the context otherwise requires, other words or expressions contained in these articles bear the same meaning as in the Model Articles and CA 2006, in each case as in force on the date when these articles become binding on the Company.

1.3 For the purposes of these articles a corporation shall be deemed to be present in person if its representative duly authorised in accordance with the Companies Acts is present in person.

1.4 Headings in these articles are used for convenience only and shall not affect the construction or interpretation of these articles.

1.5 A reference in these articles to an "article" is a reference to the relevant article of these articles unless expressly provided otherwise.

1.6 Unless expressly provided otherwise, a reference to a statute, statutory provision or subordinate legislation is a reference to it as it is in force from time to time, taking account of:

(a) any subordinate legislation from time to time made under it; and

(b) any amendment or re-enactment,

and includes any statute, statutory provision or subordinate legislation which it amends or re-enacts.

1.7 Any phrase in these articles or the Model Articles introduced by the terms "including", "include", "in particular" or any similar expression shall be construed as illustrative and shall not limit the sense of the words preceding those terms.

2. Adoption and variation of Model Articles

2.1 Subject as provided in these articles, the Model Articles shall apply to the Company.

2.2 Model Articles 7, 8(2), 11, 12, 13(3), 16, 17(2), 18(4), 19, 20, 21, 23, 41, 52 – 62 (inclusive), and 70 – 77 (inclusive) shall not apply to the Company.

3. Conflicts of interest

3.1 In this article and articles 4 and 5:

"**authorise**" means to authorise in accordance with section 175(5)(a) CA 2006 and "**authorisation**", "**authorised**" and cognate expressions shall be construed accordingly;

a "**conflict of interest**" includes a conflict of interest and duty and a conflict of duties;

"**conflicted director**" means a director in relation to whom there is a conflicting matter;

"**conflicting matter**" means a matter which would or might (if not authorised or if not permitted under article 4) constitute or give rise to a breach of the duty of a director under section 175(1) CA 2006 to avoid a conflict situation;

"**conflict situation**" means a situation in which a director has, or can have, a direct or indirect interest that conflicts, or possibly may conflict, with the interests of the company (including a conflict of interest);

"**interested director**" means a director who has, in any way, a material direct or indirect interest in a matter or decision;

a conflicting matter, conflict situation or interest is "**material**" unless it cannot reasonably be regarded as likely to give rise to a conflict of interest; and

"**other directors**" means, in relation to a particular conflicting matter, directors who are not interested directors in relation to that conflicting matter.

3.2 Exercise of the power of the directors to authorise a conflicting matter shall be subject to the provisions of this article.

3.3 The provisions of this article apply:

(a) subject to article 4; and

(b) without prejudice (and subject) to the provisions of section 175(6) CA 2006.

Nothing in these articles shall invalidate an authorisation.

3.4 A conflicted director seeking authorisation of any conflicting matter shall disclose to the other directors the nature and extent of the conflicting matter as soon as is reasonably practicable. The conflicted director shall provide the other directors with such details of the conflicting matter as are necessary for the other directors to decide how to address the conflicting matter, together with such additional information as may be requested by the other directors.

3.5 Any director (including the conflicted director) may propose that a conflicted director's conflicting matter be authorised. Any such proposal, and any authorisation given by the directors, shall be effected in the same way as any other matter that may be proposed to and resolved on by the directors under the provisions of these articles, except that:

(a) the conflicted director and any other interested director shall not count towards the quorum nor vote on any resolution giving that authorisation; and

(b) the conflicted director and any other interested director may, if the other directors so decide, be excluded from any meeting of the directors while the conflicting matter and the giving of that authorisation are under consideration.

3.6 Where the directors authorise a conflicted director's conflicting matter:

(a) the directors may (whether at the time of giving the authorisation or subsequently):

(i) require that the conflicted director is excluded from the receipt of information, the participation in discussions and/or the making of decisions (whether at meetings of the directors or otherwise) in relation to which any actual or potential conflict of interest may arise from the conflicting matter; and

(ii) impose on the conflicted director such other terms or conditions for the purpose of dealing with any actual or potential conflict of interest which may arise from the conflicting matter as they may determine;

(b) the conflicted director shall conduct himself in accordance with any terms or conditions imposed by the directors (whether at the time of giving that authorisation or subsequently);

(c) the directors may provide that, where the conflicted director obtains (otherwise than through his position as a director) information that is confidential to a third party, the conflicted director will not be obliged to disclose the information to the company, or to use or apply the information in relation to the company's affairs, where to do so would amount to a breach of that confidence;

(d) the terms of the authorisation shall be recorded in writing (but the authorisation shall be effective whether or not the terms are so recorded); and

(e) the directors may revoke or vary the authorisation at any time but no such action will affect anything done by the conflicted director prior to that action in accordance with the terms of the authorisation.

4. Permitted conflict situations

4.1 If a director or a connected person of a director:

(a) is or becomes a member, director, manager or employee of the company or any other Group Company; or

(b) acquires and holds shares in the capital of any other body corporate, wherever incorporated, provided that the shares held by the director and his connected persons do not exceed 3% of the nominal value of the issued share capital of that body corporate;

any conflict situation which arises only by reason of such a conflicting matter is permitted by this article and the relevant conflicting matter does not require disclosure and authorisation in accordance with article 3.

4.2 A director shall not, by reason of his office or of the resulting fiduciary relationship, be liable to account to the company for any benefit which he (or a person connected with him) derives from:

(a) a conflicting matter authorised by the directors;

(b) a conflicting matter to which article 4.1 applies; or

(c) a decision of the directors in relation to which, in accordance with article 5.2, the director was an eligible director, notwithstanding his relevant conflicting interest,

and no transaction or arrangement shall be liable to be avoided on the grounds of any such interest or benefit.

5. Directors' interests and decision making

5.1 Model Articles - 8 – 10 (inclusive), 13, 17 and 18 shall take effect subject to the terms of the Code.

5.2 A director who has a direct or indirect interest or duty that conflicts with the interests of the company in relation to a proposed decision of the directors is not an eligible director in relation to that decision unless article 5.3 applies to him.

5.3 A director who has a direct or indirect interest that conflicts with the interests of the company in relation to a proposed decision of the directors (a "relevant conflicting interest") shall be an eligible director in relation to that decision, provided that:

(a) in a case where the relevant conflicting interest is in an actual or proposed transaction or arrangement with the company, the nature and extent of the relevant conflicting interest either:

(i) has been duly declared to the other directors in accordance with section 177 or section 182 CA 2006, as the case may require; or

(ii) is not required by the terms of either of those sections to be declared; and

(A) where the relevant conflicting interest is constituted by, or arises from, a conflicting matter of the director and:

(1) that conflicting matter (or any breach of the relevant director's duty under section 175(1) CA 2006 by reason of that conflicting matter) is or has been authorised, permitted, approved or ratified, either in accordance with article 3 or article 4 or by the members (and that authorisation, permission, approval or ratification has not been revoked, withdrawn or reversed); and

(2) the relevant director has not been required to be excluded from participation in discussions

and/or the making of decisions in relation to which the director has the relevant conflicting interest; or

(B) where the relevant conflicting interest is constituted by, or arises from, a conflicting matter of the director and that conflicting matter (or any breach of the relevant director's duty under section 175(1) CA 2006 by reason of that conflicting matter) is not or has not been authorised, permitted, approved or ratified, either in accordance with article 3 or article 4 or by the members:

(1) the conflict situation arising by reason of that conflicting matter is not material; or

(2) the other directors are aware of the relevant conflicting interest and have determined that the director shall be an eligible director in relation to that decision; and

(b) in any other case:

(i) the director has disclosed the nature and extent of the relevant conflicting interest, or has not done so where:

(A) it cannot reasonably be regarded as likely to give rise to a conflict of interest; or

(B) the other directors are already aware of it; and

(ii) where the relevant conflicting interest is constituted by, or arises from, a conflicting matter of the director and:

(A) that conflicting matter (or any breach of the relevant director's duty under section 175(1) CA 2006 by reason of that conflicting matter) is or has been authorised, permitted, approved or ratified, either in accordance with article 3 or article 4 or by the members (and that authorisation, permission, approval or ratification has not been revoked, withdrawn or reversed); and

(B) the relevant director has not been required to be excluded from participation in discussions and/or the making of decisions in relation to which the director has the relevant conflicting interest; or

(iii) where the relevant conflicting interest is constituted by, or arises from, a conflicting matter of the director and that conflicting matter (or any breach of the relevant director's duty under section 175(1) CA 2006 by reason of that conflicting matter) is not or has not been authorised, permitted, approved or ratified, either in accordance with article 3 or article 4 or by the members:

(A) the conflict situation arising by reason of that conflicting matter is not material; or

(B) the other directors are aware of the relevant conflicting interest and have determined that the director shall be an eligible director in relation to that decision; but

the provisions of this article do not apply in relation to a decision under article 3.5.

For the purposes of this article, the other directors are to be treated as aware of anything of which they ought reasonably to be aware.

5.4 If a question arises at a meeting of the directors about whether or not a director (other than the chair of the meeting):

(a) has a material conflict situation for the purposes of articles 3 or 4;

(b) can vote (where that director does not agree to abstain from voting) on the issue in relation to which the conflict situation arises; or

(c) can be counted in the quorum (where that director does not agree not to be counted in the quorum) for the purpose of voting on the issue in relation to which the conflict arises,

the question must (unless article 5.5 applies) be referred to the chair of the meeting. The ruling of the chair of the meeting in accordance with this article 5.4 about any director other than himself is final and conclusive, unless the nature or extent of the director's conflict situation (so far as it is known to him) has not been fairly disclosed to the other directors.

5.5 If in relation to a question of the kind referred to in article 5.4 the chair of the meeting is an interested director, the question must be referred to the other directors in accordance with article 5.5 as if it were a question about the chair of the meeting.

5.6 If a question of the kind referred to in article 5.4 arises about the chair of the meeting (or if article 5.5 applies), the question shall be decided by a resolution of the other directors. The chair of the meeting (or conflicted director) cannot vote on the question but can be counted in the quorum. The other directors' resolution about the chair of the meeting (or conflicted director) is conclusive, unless the nature and extent of the chair's (or conflicted director's) conflict situation (so far as it is known to him) has not been fairly disclosed to the other directors.

5.7 For the purposes of:

(a) any meeting (or part of a meeting) held in accordance with article 3 to authorise a director's conflict; or

(b) any determination in accordance with article 5.4 or 5.6,

if there is only one director present who is not an interested director for the purpose of that authorisation or determination, the quorum for that meeting (or part of a meeting) is one eligible director.

5.8 For the purposes of:

(a) any written directors' resolution to authorise a director's conflict in accordance with article 3; or

(b) any written determination in accordance with article 5.4 or 5.6,

if there is only one director in office who is not an interested director for the purpose of that authorisation or determination, the quorum for the purpose of signing that resolution or determination is one eligible director.

5.9 Nothing in this article 5 shall be taken as absolving any director from any of the obligations set out in article 3. A determination by the directors in accordance with article 5.3(a)(ii)(B)(2) or 5.3(b)(iii)(B) that a conflicted director may be an eligible director in relation to a decision of the directors does not amount to authorisation of the relevant conflict situation.

5.10 The company may, by ordinary resolution, ratify any transaction, arrangement or other matter which has not been properly authorised by reason of a contravention of these articles.

6. Decision-making by directors: general

6.1 Subject to the terms the Code, the general rule about decision-making by directors is that any decision of the directors must be either a majority decision at a meeting or by written resolution in accordance with Model Article 18.

6.2 The quorum for each meeting of the Board is one half of all Directors appointed at the relevant time, at least one of whom must be the SECCo Chair (or his or her alternate as such). If:

(a) the Company only has one director; and

(b) no other provision of these articles requires it to have more than one director,

the general rule does not apply, the quorum for meetings of the directors shall be one and the director may take decisions without regard to any of the provisions of these articles relating to directors' decision-making, other than the provisions of articles 6.3 and 6.7.

6.3 The directors must ensure that the Company keeps a record, in writing, for at least 10 years from the date of the decision recorded, of every unanimous or majority decision taken by the directors.

6.4 Model Article 9(3) shall be modified so that any meeting where all the directors participating are not in the same place shall be treated as taking place in the place where the chair of the meeting is.

6.5 Model Article 10(2) shall be read:

(a) subject to articles 5 and 6.2; and

(b) as if the final word was deleted and the words "two eligible directors" were added in its place.

6.6 The chair of directors' meetings shall have no vote, save in the event of an equality of votes, where he shall have a casting vote, and Model Article 13(2) shall be modified accordingly.

6.7 Model Article 14(2) shall be read as if the words "to be counted" to "voting purposes" inclusive were omitted and the words "an eligible director for the purposes of that meeting (or part of a meeting)" were added in their place.

6.8 For the purposes of Model Articles 17 and 18, a written resolution of the directors may be in electronic form. Model Article 18 shall be read as if the words "all the directors" were omitted and the words "a simple majority of the directors" were added in their place.

6.9 A decision may not be taken in accordance with Model Article 18 if the eligible directors making that decision would not have formed a quorum at a directors' meeting resolving on the same matter.

6.10 Save for the chair person, the directors shall not be entitled to any remuneration from the Company. This is without prejudice to the recovery of reasonable expenses properly incurred in connection with the Company.

7. General meetings and written resolutions

7.1 Voting rights attaching to a share may be exercised, either at a general meeting or on any written resolution, notwithstanding that amounts are outstanding, due and payable to the Company in respect of that share.

8. Allotment of shares

8.1 Without prejudice to any special rights previously conferred on the holders of any existing shares or class of shares, all shares shall be issued to the persons, on the terms and conditions and with the rights, priorities, privileges or restrictions in each case as provided in the resolution creating or issuing the relevant shares. In the absence of any such provision, the directors may issue the shares, subject to section 551 CA 2006, to such persons at such times and generally on such terms and conditions and with such rights, priorities, privileges or restrictions as they may think fit. Accordingly, and in accordance with section 570 CA 2006, sections 561(1) and 562 CA 2006 shall not apply to the Company.

8.2 No share shall be issued to any infant, bankrupt, insolvent body corporate or person who, by reason of that person's mental health, is subject to a court order which wholly or partly prevents that person from personally exercising any powers or rights which that person would otherwise have.

9. Transmission of shares

9.1 Nothing in these articles or the Model Articles releases the estate of a deceased member from any liability in respect of a share solely or jointly held by that member.

10. Return of capital

10.1 The Shareholders intend that the Company should be run on a "break even" basis and shall procure that any surplus working capital shall, rather than being distributed to Shareholders, be retained by the Company and applied to subsequent expenditure.

10.2 Subject to articles 10.1 and 10.3, on a return of capital on liquidation, capital reduction or otherwise, the surplus assets of the Company remaining after the payment of its liabilities shall be applied:

(a) in paying to each holder of shares an amount in respect of each share held equal to the amount paid up thereon (including any premium); and

(b) thereafter, in distributing the balance of such assets amongst the holders of the shares in proportion to the amounts paid up or credited as paid up on the shares and held by them.

10.3 Any Shareholder may elect (by notice to the Company secretary) to pay up all amounts which remain unpaid on any Share immediately prior to any return of capital of the kind referred to in article 10.2.

11. Delivery of documents and information

11.1 Any notice, document or other information shall be deemed to be served on and delivered to the intended recipient:

(a) if properly addressed and sent by prepaid United Kingdom first class post to an address in the United Kingdom, 48 hours after it was posted (or five business days after posting either to an address outside the United Kingdom or from outside the United Kingdom to an address within the United Kingdom, if (in each case) sent by reputable international overnight courier addressed to the intended recipient, provided that delivery in at least five business days was guaranteed at the time of sending and the sending party receives a confirmation of delivery from the courier service provider);

(b) if properly addressed and delivered by hand, when it was given or left at the appropriate address; and

(c) if sent or supplied by means of a website, when the material is first made available on the website or (if later) when the recipient receives (or is deemed to have received) notice of the fact that the material is available on the website.

For the purposes of this article, no account shall be taken of any part of a day that is not a working day.

11.2 In proving that any notice, document or other information was properly addressed, it shall be sufficient to show that the notice, document or other information was delivered to an address permitted for the purpose by CA 2006.

11.3 For the purposes of section 1147(3) CA 2006, where a document or information is sent or supplied by the Company to any member by electronic means, and the Company is able to show that it was properly addressed, it is deemed to have been received by the intended recipient one hour after it was sent (but subject to section 1147(5)).

11.4 Where a document or information is sent or supplied to the Company by one person (the "**agent**") on behalf of another person (the "**sender**"), the Company may require reasonable evidence of the authority of the agent to act on behalf of the sender.

12. The Code

12.1 In addition to the provisions of these Articles, the members shall be obliged (except to the extent, if any, prohibited by law) to give effect to the Code in force at the relevant time.

12.2 Each Shareholder shall procure, to the extent reasonably possible, that the Directors shall act in all reasonable respects in relation to the Company so as to give effect to the Code, provided always that each Director will not be required to act in any manner prejudicial to his fiduciary duties as a Director of the Company.

SEC SCHEDULE 5 – ACCESSION INFORMATION

1. The Applicant’s full name.

2. Whether the Applicant is a company or a natural person or a partnership etc.

3. The Applicant’s jurisdiction of incorporation (if applicable).

4. The Applicant’s registered number (if applicable).

5. The Applicant’s registered address (or, if not applicable, its principal address).

6. Where the Applicant is incorporated or resident outside Great Britain, an address in Great Britain for the receipt of legal notices on the Applicant’s behalf.

7. The Applicant’s VAT registration number (if applicable).

8. The Applicant’s address for invoices under the Code.

9. The Applicant’s address or addresses for all other notices under the Code.

10. The Party Category into which the Applicant considers it will initially fall.

11. The Energy Licences held by the Applicant (including any for which it has applied).

12. Details of any Parties that are Affiliates of the Applicant (where the Applicant is a company).

13. Where the Applicant holds one or more Energy Supply Licences, details of the unique identifiers by which the Applicant is identified under the BSC and/or the UNC (as applicable) for the purposes of recording the Applicant's Registration for an MPAN or MPRN.

14. Where the Applicant holds an Electricity Distribution Licence or a Gas Transporter Licence, details of the unique identifier by which the Applicant is identified under the BSC and/or the UNC (as applicable) for the purposes of recording the network to which an MPAN or MPRN relates.

15. Where applicable, details of the unique identifiers by which the Applicant is identified as a Meter Operator or a Meter Asset Manager for an MPAN or MPRN.

16. The name of the person or persons who will enter into the Accession Agreement on behalf of the Applicant.

SEC SCHEDULE 6 - FORM OF LETTER OF CREDIT

Form of Document: Irrevocable Standby Letter of Credit

Documentary Credit Number: []

Date of Issue: [ ]

Issuing Bank: []

At the request of the Applicant, the Issuing Bank issues this irrevocable standby letter of credit ("**Standby Letter of Credit**") in the Beneficiary's favour on the following terms and conditions.

In this Standby Letter of Credit:

"**Applicant**" means [insert User's name]

"**Beneficiary**" means [DCC] [insert company number and address], and its successors as the DCC under the Smart Energy Code

"Beneficiary Statement" means a demand on the Beneficiary's letterhead, stating the name and title of the person signing on behalf of the Beneficiary, in the form set out at in the schedule to this Standby Letter of Credit.

"**Effective Date**" means [ ] (London, UK)

"**Expiry Date**" means [ ] (London, UK)

"**Maximum Amount**" means []

"**Smart Energy Code**" means the code of that name designated by the Secretary of State pursuant to the smart meter communication licences granted pursuant to the Electricity Act 1989 and the Gas Act 1986, as such code is modified from time to time.

1. From the Effective Date, this Standby Letter of Credit is available for payment at sight against presentation to the Issuing Bank of a Beneficiary Statement.

2. The Issuing Bank will not be obliged to make a payment under this Standby Letter of Credit if as a result the aggregate of all payments made by it under this Standby Letter of Credit would exceed the Maximum Amount.

3. The Beneficiary Statement must be presented to the Issuing Bank on or before the Expiry Date.

4. All payments under this Letter of Credit shall be made in Pounds Sterling in immediately available, freely transferable funds and for value on the due date to the account set out in the Beneficiary Statement.

5. The Issuing Bank hereby waives any right to set off or counterclaim whatsoever against any amounts payable under this Standby Letter of Credit in respect of any claims the Issuing Bank may have against the Beneficiary and such amounts shall be paid free and clear of all deductions or withholdings whatsoever. If the Issuing Bank is required by law to make a tax deduction from any amounts payable under this Standby Letter of Credit, the amount due from the Issuing Bank shall be increased to an amount which (after such tax deduction) leaves an amount equal to the payment which would have been due if no tax deduction had been required.

6. This Standby Letter of Credit is personal to the Beneficiary, and the Beneficiary's rights hereunder (including the right to receive proceeds) are not assignable; provided that such rights shall enure for the benefit of the DCC's successors under the Smart Energy Code.

7. Except to the extent it is inconsistent with the express terms of this Standby Letter of Credit, this Standby Letter of Credit is subject to the Uniform Customs and Practice for Documentary Credits (2007 Revision), International Chamber of Commerce Publication No. 600 other than Article 38 thereof which is hereby waived and Article 36 is varied as below. Other than a person to whom this Standby Letter of Credit has been transferred in accordance with clause 6, this Standby Letter of Credit shall not confer any benefit on or be enforceable by any third party. If this Standby Letter of Credit expires during any interruption of business as described in Article 36 of said Publication 600, the Issuing Bank specifically agrees to honour any demand made under this Standby Letter of Credit within thirty (30) days after the resumption of business.

8. This Standby Letter of Credit and any non-contractual obligations or disputes arising out of or in connection with it shall be governed by and construed in accordance with the laws of England and the parties submit to the exclusive jurisdiction of the Courts of England for all disputes arising under, out of, or in relation to this Letter of Credit.

Signed for and on behalf of

Issuing Bank

Schedule - Form of Beneficiary Statement

We, the DCC under the Smart Energy Code (the “Beneficiary”), hereby state that we are entitled, in accordance with the Smart Energy Code, to demand ……….[insert amount being claimed] under Standby Letter of Credit number……..... issued by …………[insert name of Issuing Bank]. Payment in respect of this demand shall be effected immediately to [insert relevant account details]. We confirm that the signatory(ies) to this demand are empowered to sign and make this demand on behalf of the Beneficiary.

SEC SCHEDULE 7 – SPECIMEN ENABLING SERVICES AGREEMENT

Dated:2[XXX]

[Participant]

and

[DCC]

Smart Energy Code
Enabling Services
Agreement

THIS ENABLING SERVICE AGREEMENT is made on 2[XXX]

BETWEEN:

(1). [**TBC**] a company incorporated in [*Jurisdiction*] (registered number [TBC]) whose registered office is at [TBC] (the "**Participant**"); and

(2). [**TBC**] a company incorporated in [*Jurisdiction*] (registered number [TBC]) whose registered office is at [TBC] (the "**DCC**").

WHEREAS

(A). The Participant wishes to procure the Enabling Services pursuant to the Smart Energy Code.

(B). The DCC has agreed to provide the Enabling Services pursuant to this Enabling Services Agreement, in consideration of the Enabling Service Charges.

NOW IT IS HEREBY AGREED as follows:

1. Interpretation

1.1 In this Enabling Services Agreement, unless the context otherwise requires:

"**Enabling Service Charges**" means those charges described in Schedule 2.

"**Enabling Services**" means the services described in Schedule 1.

"**Event of Default**" means that the Participant:

(a) is in material breach of any of its material obligations under this Enabling Services Agreement, and the Participant has failed to remedy the breach within 20 Working Days after a notice from the DCC requiring such remedy; and/or

(b) suffers an Insolvency Type Event.

"**Party**" means the DCC or the Participant; and "**Parties**" means both of them.

"**Smart Energy Code**" means the code of that name designated by the Secretary of State pursuant to the smart meter communication licences granted to the DCC pursuant to the Electricity Act 1989 and the Gas Act 1986, as such code is modified from time to time in accordance with its provisions.

1.2 In this Enabling Services Agreement, unless the context otherwise requires, references to "Clauses" and "Schedules" are to the clauses of, and schedules to, this Enabling Services Agreement.

1.3 Subject to Clauses 1.1 and 1.2, the words and expressions used in this Enabling Services Agreement shall be construed and interpreted in accordance with the definitions and provisions regarding interpretation set out in Section A (Definitions and Interpretation) of the Smart Energy Code, as if:

(a) those definitions and provisions regarding interpretation were set out in this Enabling Services Agreement;

(b) the uses therein of the words defined in Clause 1.1 were interpreted in accordance with Clause 1.1; and

(c) the references therein to:

(i) "Charges" were to "Enabling Service Charges";

(ii) "Services" were to "Enabling Services";

(iii) "User" were to "Participant"; and

(iv) "this Code" or "this Code and/or any Bilateral Agreement" were to "this Enabling Services Agreement".

1.4 The Parties acknowledge that the Smart Energy Code is subject to modification from time to time in accordance with its provisions and law, and that the Smart Energy Code as so modified from time to time shall apply for the purposes of this Enabling Services Agreement.

1.5 References in this Enabling Services Agreement (or in provisions incorporated herein by reference) to Sections of the Smart Energy Code shall be to those sections as incorporated into this Enabling Services Agreement, as such sections are modified and/or renumbered from time to time.

2. Commencement of this Enabling Services Agreement

2.1 This Enabling Services Agreement shall commence on [TBC].

3. Provision of the Enabling Services

3.1 The DCC shall provide the Enabling Services to the Participant subject to and in accordance with this Enabling Services Agreement.

3.2 The DCC and the Participant shall each comply with the additional obligations assigned to them in Schedule 1.

4. Enabling Service Charges

4.1 The Participant shall pay the Enabling Service Charges in respect of which Sections J1 (Payment of Charges) and J2 (Payment Default and Disputes) shall apply as if:

(a) those Sections were set out in this Enabling Services Agreement;

(b) the uses therein of the words defined in Clause 1.1 were interpreted in accordance with Clause 1.1;

(c) the references therein to expressions referred to in Clause 1.3(c) were interpreted as referred to in that Clause; and

(d) Section J2.7 (Pursing Non-Payment) did not apply.

5. Limitations of Liability

5.1 The DCC's and the Participant's liability under or in connection with this Enabling Services Agreement shall be limited in accordance with Section M2 (Limitations of Liability) as if:

(a) that Section was set out in this Enabling Services Agreement;

(b) the uses therein of the words defined in Clause 1.1 were interpreted in accordance with Clause 1.1;

(c) the references therein to expressions referred to in Clause 1.3(c) were interpreted as referred to in that Clause; and

(d) Sections M2.17 and M2.18 (SECCo) did not apply.

6. Termination or Expiry of this Enabling Services Agreement

6.1 Subject to earlier termination in accordance with this Clause 6, this Enabling Services Agreement shall expire on [TBC].

6.2 The Participant shall, at its discretion, be entitled to terminate this Enabling Services Agreement on 20 Working Days' prior notice in writing to the DCC.

6.3 The DCC shall be entitled to immediately terminate this Agreement on notice to the Participant where an Event of Default occurs.

6.4 The expiry or earlier termination of this Agreement shall be without prejudice to:

(a) those rights and obligations under this Enabling Services Agreement that may have accrued prior to such expiry or termination; or

(b) those provisions of this Enabling Services Agreement that are expressly or by implication intended to survive such expiry or termination, including Clauses 4 and 5.

7. Amendments

7.1 Without prejudice to Clause 1.4, this Enabling Services Agreement may only be amended by agreement in writing by the Parties or in order to give effect to any determination of disputes by the Authority pursuant to the DCC Licence.

7.2 The Parties shall amend this Enabling Services Agreement where it has become inconsistent with the Smart Energy Code in order to correct such inconsistency (including where the Specimen Enabling Services Agreement is modified, in which case the Parties shall amend this Enabling Services Agreement in the same manner and to the same extent).

7.3 The Participant hereby authorises the DCC to make the amendments to this Enabling Services Agreement required pursuant to Clause 7.2 on the Participant's behalf. Where the Participant disputes the requirement for, or form of, any such amendments made by the DCC on the Participant's behalf, then the Participant may refer the matter to the Panel for its determination. Nothing in this Clause 7.3 shall fetter the Participant's right to refer disputes to the Authority pursuant to the DCC Licence.

8. Miscellaneous

8.1 The Parties agree that the provisions of Sections M3 (Services FM and Force Majeure), M4 (Confidentiality), M7 (Dispute Resolution), M9 (DCC Transfer), M10 (Notices) and M11 (Miscellaneous) of the Smart Energy Code shall apply to this Enabling Services Agreement, as if:

(a) those Sections were set out in this Enabling Services Agreement;

(b) the uses therein of the words defined in Clause 1.1 were interpreted in accordance with Clause 1.1;

(c) the references therein to expressions referred to in Clause 1.3(c) were interpreted as referred to in that Clause; and

(d) the following Sections did not apply: Sections M3.14 (SECCo), M7.16 (SECCo), M10.1 (Communication via Specified Interfaces), M10.6 (The Panel, Code Administrator, Secretariat and SECCo), M11.5 (Third Party Rights), and M11.15 (SECCo).

8.2 This Enabling Services Agreement may be executed in any number of counterparts, each of which shall be an original but all of which together shall constitute one and the same instrument.

9. Governing Law

9.1 In accordance with Clause 8, this Enabling Services Agreement and any dispute or claim arising out of or in connection with it (including non-contractual claims) shall be governed by, and construed in accordance with, the relevant laws specified in Section M11 (Miscellaneous) of the Smart Energy Code from time to time for the purpose of disputes or claims of that nature.

THIS ENABLING SERVICES AGREEMENT has been entered into on the date first stated above.

SIGNED by

duly authorised for and on behalf of ………………………………………..

……………………………………….. *Print name of person signing*

Print full name of Participant

Signature …………………………………………

SIGNED by

duly authorised for and on behalf of the DCC ………………………………………..

Print name of person signing

Signature …………………………………………

Schedule 1 – Enabling Services

[The Enabling Services shall comprise the provision of Test Communications Hubs in accordance with Section F10 (Test Communications Hubs). The DCC and the Participant shall each comply with their respective obligations set out or referred to in that Section F10 (the Participant complying with those obligations assigned to TCH Participants).]

[The Enabling Services shall comprise the provision of either or both those Device and User System Tests described in Section H14.31(a) and (b) (Device and User System Tests) in accordance with Section H14 (Testing Services). The DCC and the Participant shall each comply with their respective obligations set out or referred to in that Section H14 (the Participant complying with those obligations assigned to Testing Participants).]

[The Enabling Services shall comprise the provision of SMETS1 Pending Product Combinations Tests in accordance with Section H14 (Testing Services). The DCC and the Participant shall each comply with their respective obligations set out or referred to in that Section H14 (the Participant complying with those obligations assigned to Testing Participants).]

[The Enabling Services shall comprise the provision of RF Noise Testing in accordance with Section H14 (Testing Services). The DCC and the Participant shall each comply with their respective obligations set out or referred to in that Section H14 (the Participant complying with those obligations assigned to Testing Participants).]

[The Enabling Services shall comprise the provision of Interoperability and Innovation Events in accordance with Section H14 (Testing Services). The DCC and the Participant shall each comply with their respective obligations set out or referred to in that Section H14 (the Participant complying with those obligations assigned to Testing Participants).]

[The Enabling Services shall comprise the provision of GFI Testing in accordance with Section H14 (Testing Services). The DCC and the Participant shall each comply with their respective obligations set out or referred to in that Section H14 (the Participant complying with those obligations assigned to Testing Participants).]

[The Enabling Services shall comprise the provision of DCC Boxed in accordance with Section H14 (Testing Services). The DCC and the Participant shall each comply with their respective obligations set out or referred to in that Section H14 (the Participant complying with those obligations assigned to Testing Participants).]

[The Enabling Services shall comprise the provision of MAP/Manufacturer Reports in accordance with Section H17 (MAP/Manufacturer Reports). The DCC and the Participant shall each comply with their respective obligations set out or referred to in that Section H17.]

Schedule 2 – Enabling Service Charges

The Enabling Service Charges shall comprise those charges set out in the Charging Statement from time to time that apply to the Explicit Charging Metrics (as defined in the Charging Methodology) that comprise the Enabling Services, being the Explicit Charge applicable to the:

[ordering of Test Communications Hubs pursuant to Section F10 (Test Communications Hubs)] / [the provision of a connection to the SM WAN pursuant to Section H14.31 (Device and User System Testing)] / [the provision of additional testing support pursuant to Section H14.33 (Device and User System Testing)].

SCHEDULE 8 – GREAT BRITAIN COMPANION SPECIFICATION

[Please use this placeholder to download your required version of SEC Schedule 8 'Great Britain Companion Specification']

Download SEC Schedule 8 'GB Companion Specification' version 1.0 here.

Download SEC Schedule 8 'GB Companion Specification' version 1.1 here.

Download SEC Schedule 8 'GB Companion Specification' version 2.0 here.

Download SEC Schedule 8 'GB Companion Specification' version 2.1 here.

Download SEC Schedule 8 'GB Companion Specification' version 3.0 here.

Download SEC Schedule 8 'GB Companion Specification' version 3.1 here.

Download SEC Schedule 8 'GB Companion Specification' version 3.2 here.

Download SEC Schedule 8 'GB Companion Specification' version 3.3 here.

Download SEC Schedule 8 'GB Companion Specification' version 4.0 here.

Download SEC Schedule 8 'GB Companion Specification' version 4.1 here.

Download SEC Schedule 8 'GB Companion Specification' version 4.2 here.

Download SEC Schedule 8 'GB Companion Specification' version 4.3 here.

SCHEDULE 9 – SMART METERING EQUIPMENT TECHNICAL SPECIFICATIONS

[Please use this placeholder to download your required version of SEC Schedule 9 'Smart Metering Equipment Technical Specifications']

Download SEC Schedule 9 'Smart Metering Equipment Technical Specifications 1' - 1 February 2018 here.

Download SEC Schedule 9 'Smart Metering Equipment Technical Specifications 2' - 1 February 2018 here.

Download SEC Schedule 9 'Smart Metering Equipment Technical Specifications 2' - 8 November 2018 here.

Download SEC Schedule 9 'Smart Metering Equipment Technical Specifications 2' - 4 July 2019 here.

Download SEC Schedule 9 'Smart Metering Equipment Technical Specifications 2' - 29 November 2020 here.

Download SEC Schedule 9 'Smart Metering Equipment Technical Specifications 2' - 4 November 2021 here.

Download SEC Schedule 9 'Smart Metering Equipment Technical Specifications 2' - 3 November 2022 here.

Download SEC Schedule 9 'Smart Metering Equipment Technical Specifications 2' - 2 November 2023 here.

SCHEDULE 10 – COMMUNICATIONS HUB TECHNICAL SPECIFICATIONS

[Please use this placeholder to download your required version of SEC Schedule 10 'Communications Hub Technical Specifications']

Download SEC Schedule 10 'Communications Hub Technical Specifications' version 1.0 here.

Download SEC Schedule 10 'Communications Hub Technical Specifications' version 1.1 here.

Download SEC Schedule 10 'Communications Hub Technical Specifications' version 1.2 here.

Download SEC Schedule 10 'Communications Hub Technical Specifications' version 1.3 here.

Download SEC Schedule 10 'Communications Hub Technical Specifications' version 1.4 here.

Download SEC Schedule 10 'Communications Hub Technical Specifications' version 1.5 here.

Download SEC Schedule 10 'Communications Hub Technical Specifications' version 1.6 here.

TS Version Lookup Table

The following Table provides a cross reference to indicate which of the SEC Schedule 9 (SMETS) documents contain which Versions of the Device Technical Specifications.

Technical Specification Cross Reference	SMETS1 1 February 2018	SMETS2 1 February 2018	SMETS2 8 November 2018	SMETS2 4 July 2019	SMETS2 29 November 2020	SMETS2 4 November 2021	SMETS2 3 November 2022	SMETS2 2 November 2023
GSMETS	(GSMS) 1.2	2.0	3.1	4.2	4.3	4.3	4.4	4.5
ESMETS	(ESMS) 1.2	2.0	3.1	4.2	5.0	5.1	5.2	5.2
IHDTS	1.2	2.0	3.1	4.2	4.3	4.3	4.4	4.4
PPMIDTS	N/A	2.0	3.1	4.2	4.3	4.4	4.5	4.5
HCALCSTS	N/A	2.0	3.1	4.2	5.0	5.1	5.1	5.1
SAPCTS	N/A	N/A	N/A	N/A	5.0	5.0	5.1	5.1

TS Applicability Tables[1]

It should be noted that references to versions of specifications that can no longer be used operationally have been removed from these tables.

SMETS1 Devices: GSMSTS

GSMSTS Version	Installation Start Date	General Installation End Date	PPM Installation End Date	Maintenance Start Date	Maintenance End Date	Relevant GBCS Version	Applicability Period Start Date	Applicability Period End Date
1.2	18/12/12	05/12/18	15/03/19	18/12/12	Not determined	Not applicable	Not applicable	Not applicable

SMETS1 Devices: ESMSTS

ESMSTS Version	Installation Start Date	General Installation End Date	PPM Installation End Date	Maintenance Start Date	Maintenance End Date	Relevant GBCS Version	Applicability Period Start Date	Applicability Period End Date
1.2	18/12/12	05/12/18	15/03/19	18/12/12	Not determined	Not applicable	Not applicable	Not applicable

SMETS1 Devices: IHDTS

IHDTS Version	Installation Start Date	General Installation End Date	PPM Installation End Date	Maintenance Start Date	Maintenance End Date	Relevant GBCS Version	Applicability Period Start Date	Applicability Period End Date
1.2	18/12/12	05/12/18	15/03/19	18/12/12	Not determined	Not applicable	Not applicable	Not applicable

SMETS2+ Devices: GSMETS and Relevant Versions of GBCS

GSMETS Version	Installation Start Date	Installation End Date	Maintenance Start Date	Maintenance End Date	Relevant GBCS Version	Applicability Period Start Date	Applicability Period End Date
2.0	30/09/16	27/04/24	30/09/16	Not determined	1.1	06/11/17	Not determined
3.1	08/11/18	27/04/24	08/11/18	Not determined	2.0	28/10/18	Not determined
3.1	08/11/18	27/04/24	08/11/18	Not determined	2.1	28/10/18	Not determined
4.2	29/11/19	Not determined	29/11/19	Not determined	3.2	29/11/19	Not determined
4.2	03/11/22	Not determined	03/11/22	Not determined	3.3	03/11/22	Not determined
4.3	29/11/20	Not determined	29/11/20	Not determined	3.2	29/11/20	Not determined
4.3	03/11/22	Not determined	03/11/22	Not determined	3.3	03/11/22	Not determined
4.3	29/11/20	Not determined	29/11/20	Not determined	4.0	29/11/20	Not determined
4.3	04/11/21	Not determined	04/11/21	Not determined	4.1	04/11/21	Not determined
4.4	03/11/22	Not determined	03/11/22	Not determined	4.2	03/11/22	Not determined
4.5	02/11/23	Not determined	02/11/23	Not determined	4.3	02/11/23	Not determined

SMETS2+ Devices: ESMETS and Relevant Versions of GBCS

ESMETS Version	Installation Start Date	Installation End Date	Maintenance Start Date	Maintenance End Date	Relevant GBCS Version	Applicability Period Start Date	Applicability Period End Date
2.0	30/09/16	27/04/24	30/09/16	Not determined	1.1	06/11/17	Not determined
3.1	08/11/18	27/04/24	08/11/18	Not determined	2.0	28/10/18	Not determined

[1] As required by SEC Section A3.33 – A3.36

3.1	08/11/18	27/04/24	08/11/18	Not determined	2.1	28/10/18	Not determined
4.2	29/11/19	Not determined	29/11/19	Not determined	3.2	29/11/19	Not determined
4.2	03/11/22	Not determined	03/11/22	Not determined	3.3	03/11/22	Not determined
5.0	29/11/20	Not determined	29/11/20	Not determined	4.0	29/11/20	Not determined
5.1	04/11/21	Not determined	04/11/21	Not determined	4.1	04/11/21	Not determined
5.2	03/11/22	Not determined	03/11/22	Not determined	4.2	03/11/22	Not determined
5.2	02/11/23	Not determined	02/11/23	Not determined	4.3	02/11/23	Not determined

SMETS2+ Devices: IHDTS and Relevant Versions of GBCS

IHDTS Version	Installation Start Date	Installation End Date	Maintenance Start Date	Maintenance End Date	Relevant GBCS Version	Applicability Period Start Date	Applicability Period End Date
2.0	30/09/16	27/04/21	30/09/16	Not determined	1.1	06/11/17	Not determined
3.1	08/11/18	27/04/21	08/11/18	Not determined	2.0	28/10/18	Not determined
3.1	08/11/18	27/04/21	08/11/18	Not determined	2.1	28/10/18	Not determined
4.2	29/11/19	Not determined	29/11/19	Not determined	3.2	29/11/19	Not determined
4.2	03/11/22	Not determined	03/11/22	Not determined	3.3	03/11/22	Not determined
4.3	29/11/20	Not determined	29/11/20	Not determined	3.2	29/11/20	Not determined
4.3	03/11/22	Not determined	03/11/22	Not determined	3.3	03/11/22	Not determined
4.3	29/11/20	Not determined	29/11/20	Not determined	4.0	29/11/20	Not determined
4.3	04/11/21	Not determined	04/11/21	Not determined	4.1	04/11/21	Not determined
4.4	03/11/22	Not determined	03/11/22	Not determined	4.2	03/11/22	Not determined
4.4	02/11/23	Not determined	02/11/23	Not determined	4.3	02/11/23	Not determined

SMETS2+ Devices: PPMIDTS and Relevant Versions of GBCS

PPMIDTS Version	Installation Start Date	Installation End Date	Maintenance Start Date	Maintenance End Date	Relevant GBCS Version	Applicability Period Start Date	Applicability Period End Date
2.0	30/09/16	27/04/24	30/09/16	Not determined	1.1	06/11/17	Not determined
3.1	08/11/18	27/04/24	08/11/18	Not determined	2.0	28/10/18	Not determined
3.1	08/11/18	27/04/24	08/11/18	Not determined	2.1	28/10/18	Not determined
4.2	29/11/19	Not determined	29/11/19	Not determined	3.2	29/11/19	Not determined
4.2	03/11/22	Not determined	03/11/22	Not determined	3.3	03/11/22	Not determined
4.3	29/11/20	Not determined	29/11/20	Not determined	3.2	29/11/20	Not determined
4.3	03/11/22	Not determined	03/11/22	Not determined	3.3	03/11/22	Not determined
4.3	29/11/20	Not determined	29/11/20	Not determined	4.0	29/11/20	Not determined
4.4	04/11/21	Not determined	04/11/21	Not determined	4.1	04/11/21	Not determined
4.5	03/11/22	Not determined	03/11/22	Not determined	4.2	03/11/22	Not determined
4.5	02/11/23	Not determined	02/11/23	Not determined	4.3	02/11/23	Not determined

SMETS2+ Devices: HCALCSTS and Relevant Versions of GBCS

HCALCSTS Version	Installation Start Date	Installation End Date	Maintenance Start Date	Maintenance End Date	Relevant GBCS Version	Applicability Period Start Date	Applicability Period End Date
2.0	30/09/16	27/04/24	30/09/16	04/11/21	1.1	06/11/17	Not determined
3.1	08/11/18	27/04/24	08/11/18	04/11/21	2.0	28/10/18	Not determined

3.1	08/11/18	27/04/24	08/11/18	04/11/21	2.1	28/10/18	Not determined
4.2	29/11/19	Not determined	29/11/19	Not determined	3.2	29/11/19	Not determined
4.2	03/11/22	Not determined	03/11/22	Not determined	3.3	03/11/22	Not determined
5.0	29/11/20	Not determined	29/11/20	Not determined	4.0	29/11/20	Not determined
5.1	04/11/21	Not determined	04/11/21	Not determined	4.1	04/11/21	Not determined
5.1	03/11/22	Not determined	03/11/22	Not determined	4.2	03/11/22	Not determined
5.1	02/11/23	Not determined	02/11/23	Not determined	4.3	02/11/23	Not determined

SMETS2+ Devices: SAPCTS and Relevant Versions of GBCS

SAPCTS Version	Installation Start Date	Installation End Date	Maintenance Start Date	Maintenance End Date	Relevant GBCS Version	Applicability Period Start Date	Applicability Period End Date
5.0	29/11/20	Not determined	29/11/20	Not determined	4.0	29/11/20	Not determined
5.0	04/11/21	Not determined	04/11/21	Not determined	4.1	04/11/21	Not determined
5.1	03/11/22	Not determined	03/11/22	Not determined	4.2	03/11/22	Not determined
5.1	02/11/23	Not determined	02/11/23	Not determined	4.3	02/11/23	Not determined

CHTS and Relevant Versions of GBCS

CHTS Version	Installation Start Date	Installation End Date	Maintenance Start Date	Maintenance End Date	Relevant GBCS Version	Applicability Period Start Date	Applicability Period End Date
1.0	30/09/16	30/04/23	30/09/16	31/05/23	1.1	06/11/17	Not determined
1.1	28/10/18	Not determined	28/10/18	Not determined	2.0	28/10/18	28/08/23
1.1	28/10/18	30/04/26	28/10/18	31/05/24	2.1	28/10/18	Not determined
1.3	29/11/19	Not determined	29/11/19	Not determined	3.2	29/11/19	Not determined
1.3	03/11/22	Not determined	03/11/22	Not determined	3.3	03/11/22	Not determined
1.4	29/11/20	Not determined	29/11/20	Not determined	4.0	29/11/20	Not determined
1.5	04/11/21	Not determined	04/11/21	Not determined	4.1	04/11/21	Not determined
1.6	03/11/22	Not determined	03/11/22	Not determined	4.2	03/11/22	Not determined
1.6	02/11/23	Not determined	02/11/23	Not determined	4.3	02/11/23	Not determined

DUIS Maintenance Validity Period

DUIS Version	Maintenance Start date	Maintenance End date
1.1	21/07/2017	26/11/2021
2.0	01/02/2018	26/11/2021
3.0	28/07/2019	TBC
3.1	29/11/2019	TBC
4.0	29/11/2020	TBC
5.0	04/11/2021	TBC
5.1	30/06/2022	TBC
5.2	29/06/2023	TBC

GBCS and Relevant Versions of CPA Security Characteristics

GBCS Version(s)	Relevant Versions of CPA Security Characteristics
• 1.0 • 1.1 • 2.0 • 2.1 • 3.2 • 3.3 • 4.0 • 4.1 • 4.2 • 4.3	The most recent Sub-Version of Principal Version 1 of the document entitled ‘CPA Security Characteristic: Smart Metering – Communications Hub’ published on the NCSC_website at the time the relevant Device Model commences the CPA Certification or re-Certification process (as applicable). The most recent Sub-Version of Principal Version 1 of the document entitled ‘CPA Security Characteristic: Electricity Smart Metering Equipment’ published on the NCSC website at the time the relevant Device Model commences the CPA Certification or re-Certification process (as applicable). The most recent Sub-Version of Principal Version 1 of the document entitled ‘CPA Security Characteristic: Gas Smart Metering Equipment’ published on the NCSC website at the time the relevant Device Model commences the CPA Certification or re-Certification process (as applicable). The most recent Sub-Version of Principal Version 1 of the document entitled ‘CPA Security Characteristic: Smart Metering – HAN Connected Auxiliary Load Control Switch’ published on the NCSC_website at the time the relevant Device Model commences the CPA Certification or re-Certification process (as applicable). The most recent Sub-Version of Principal Version 1 of the document entitled ‘CPA Security Characteristic: Smart Metering – Standalone Auxiliary Proportional Controller’ published on the NCSC website at the time the relevant Device Model commences the CPA Certification or re-Certification process (as applicable).

Version A4.0

Appendix A

Device Certificate Policy

CONTENTS

Part **Heading** **Page**

1 INTRODUCTION

The document comprising this Appendix A (together with its Annexes A and B):

- shall be known as the " **Device Certificate Policy**" (and in this document is referred to simply as the "**Policy**"),
- is a SEC Subsidiary Document related to Section L9 of the Code (The SMKI Document Set).

1.1 OVERVIEW

(A) This Policy sets out the arrangements relating to:

(i) Device Certificates; and

(ii) DCA Certificates.

(B) This Policy is structured according to the guidelines provided by IETF RFC 3647, with appropriate extensions, modifications and deletions.

(C) Except where the context otherwise requires, words or expressions used in this Policy shall have the meanings ascribed to them in IETF RFC 5280 where they:

(i) appear in `Courier New` font;

(ii) are accompanied by the descriptor 'field', 'type' or 'extension'; and/or

(iii) take the form of a conjoined string of two or more words, such as '`digitalSignature`'.

1.2 DOCUMENT NAME AND IDENTIFICATION

(A) This Policy has been assigned an OID of 1.2.826.0.1. 8641679.1.2.1.2.

1.3 SMKI PARTICIPANTS

1.3.1 The Device Certification Authority

(A) The definition of Device Certification Authority is set out in Annex A.

1.3.2 Registration Authorities

(A) The definition of Registration Authority is set out in Annex A.

1.3.3 Subscribers

(A) In accordance with Section L3 of the Code (The SMKI Services), certain Parties may become Authorised Subscribers.

(B) In accordance with Section L3 of the Code (The SMKI Services), an Authorised Subscriber shall be an Eligible Subscriber in relation to certain Certificates.

(C) The SMKI RAPP sets out the procedure to be followed by an Eligible Subscriber in order to become a Subscriber for one or more Certificates.

(D) Eligible Subscribers are subject to the applicable requirements of the SMKI RAPP and Section L11 of the Code (Subscriber Obligations).

(E) Obligations on the DCC acting in the capacity of an Eligible Subscriber are set out in Section L11 of the Code (Subscriber Obligations).

(F) The definitions of the following terms are set out in Section A of the Code (Definitions and Interpretation):

(i) Authorised Subscriber;

(ii) Eligible Subscriber;

(iii) Subscriber.

1.3.4 Subjects

(A) The Subject of a Device Certificate must be a Device (other than a Type 2 Device) represented by the identifier in the `subjectAltName` field of the Device Certificate Profile in accordance with Annex B.

(B) The Subject of a DCA Certificate must be the entity identified by the `subject` field of the Root DCA Certificate Profile or Issuing DCA Certificate Profile (as the case may be) in accordance with Annex B.

(C) The definition of Subject is set out in Annex A.

1.3.5 Relying Parties

(A) In accordance with Section L12 of the Code, certain Parties may be Relying Parties.

(B) Relying Parties are subject to the applicable requirements of Section L12 of the Code (Relying Party Obligations).

(C) Obligations on the DCC acting in the capacity of a Relying Party are set out in Section L12 of the Code.

(D) The definition of Relying Party is set out in Annex A.

1.3.6 SMKI Policy Management Authority

(A) Provision in relation to the SMKI PMA is made in Section L1 of the Code (SMKI Policy Management Authority).

1.3.7 SMKI Repository Provider

(A) Provision in relation to the SMKI Repository Service is made in Section L5 of the Code (The SMKI Repository Service).

1.4 USAGE OF DEVICE CERTIFICATES AND DCA CERTIFICATES

1.4.1 Appropriate Certificate Uses

(A) The DCA shall ensure that Device Certificates are Issued only:

(i) subject to paragraph (B), to Eligible Subscribers; and

(ii) for the purposes of the creation, sending, receipt and processing of communications to and from Devices in accordance with or pursuant to the Code.

(B) For the purposes of paragraph (A), the DCA may treat any of the following as if they were an Eligible Subscriber:

(i) in relation to a Device that has an SMI Status that is not set to ‘commissioned’ or ‘installed not commissioned’, any Authorised Subscriber; or

(ii) in relation to a Device that has an SMI Status of ‘commissioned’ or ‘installed not commissioned’, the DCC or any Authorised Subscriber that is a User which acts (or is to act) in the User Role of either Import Supplier or Gas Supplier.

(C) The DCA shall ensure that DCA Certificates are Issued only to the DCA:

(i) in its capacity as, and for the purposes of exercising the functions of, the Root DCA; and

(ii) in its capacity as, and for the purposes of exercising the functions of, the Issuing DCA.

(D) Further provision in relation to the use of Certificates is made in Section L11 (Subscriber Obligations) and Section L12 (Relying Party Obligations) of the Code.

1.4.2 Prohibited Certificate Uses

(A) No Party shall use a Certificate other than for the purposes specified in Part 1.4.1 of this Policy.

1.5 POLICY ADMINISTRATION

1.5.1 Organisation Administering the Document

(A) This Policy is a SEC Subsidiary Document and is administered as such in accordance with the provisions of the Code.

1.5.2 Contact Person

(A) Questions in relation to the content of this Policy should be addressed to the DCA or the SMKI PMA.

1.5.3 Person Determining Device CPS Suitability for the Policy

(A) Provision is made in Section L9.8 (d) of the Code for the SMKI PMA to approve the Device CPS.

1.5.4 Device CPS Approval Procedures

(A) Provision is made in Section L9.9 of the Code for the procedure by which the SMKI PMA may approve the Device CPS.

1.5.5 Registration Authority Policies and Procedures

(A) The SMKI Registration Authority Policies and Procedures (the **SMKI RAPP**) are set out at Appendix D of the Code.

1.6 DEFINITIONS AND ACRONYMS

1.6.1 Definitions

(A) Definitions of the expressions used in this Policy are set out in Section A of the Code (Definitions and Interpretation) and Annex A.

1.6.2 Acronyms

(A) Any acronyms used for the purposes of this Policy are set out in Section A of the Code (Definitions and Interpretation) and Annex A.

2 PUBLICATION AND REPOSITORY RESPONSIBILITIES

2.1 REPOSITORIES

(A) Provision is made in Section L5 of the Code (The SMKI Repository Service) for the establishment, operation and maintenance of the SMKI Repository.

2.2 PUBLICATION OF CERTIFICATION INFORMATION

(A) The DCA shall lodge copies of the following in the SMKI Repository:

(i) each Device Certificate that has been accepted by a Subscriber;

(ii) each DCA Certificate;

(iii) each version of the SMKI RAPP;

(iv) each version of the SMKI Recovery Procedure; and

(v) any other document or information that may from time to time be specified, for the purposes of this provision, by the SMKI PMA.

(B) The DCA may lodge in the SMKI Repository such other documents or information as it may from time to time consider appropriate.

(C) Further provision on the lodging of documents and information in the SMKI Repository is made in Section L5 of the Code (The SMKI Repository Service).

2.3 TIME OR FREQUENCY OF PUBLICATION

(A) The DCA shall ensure that:

(i) each Device Certificate is lodged in the SMKI Repository promptly on its acceptance by a Subscriber;

(ii) each DCA Certificate is lodged to the SMKI Repository promptly on being Issued;

(iii) the Policy is lodged in the SMKI Repository, and a revised version of the Policy is lodged in the SMKI Repository promptly following each modification to it made in accordance with the Code;

(iv) the SMKI RAPP is lodged in the SMKI Repository, and a revised version of the SMKI RAPP is lodged in the SMKI Repository promptly following each modification to it made in accordance with the Code;

(v) the SMKI Recovery Procedure is lodged in the SMKI Repository, and a revised version of the SMKI Recovery Procedure is lodged in the SMKI Repository promptly following each modification to it made in accordance with the Code; and

(vi) any other document that may from time to time be specified by the SMKI PMA is lodged in the SMKI Repository within such time as may be directed by the SMKI PMA.

2.4 ACCESS CONTROLS ON REPOSITORIES

(A) Provision in relation to access controls for the SMKI Repository is made in Sections L5.5, L5.6 and L5.6A of the Code.

3 IDENTIFICATION AND AUTHENTICATION

3.1 NAMING

3.1.1 Types of Names

(A) Provision is made in the SMKI RAPP to ensure that the name of the Subject of each Certificate is in accordance with the relevant Certificate Profile at Annex B.

3.1.2 Need for Names to be Meaningful

(A) Provision is made in the SMKI RAPP to ensure that the name of the Subject of each Certificate is meaningful and consistent with the relevant Certificate Profile in Annex B.

3.1.3 Anonymity or Pseudonymity of Subscribers

(A) Provision is made in the SMKI RAPP to:

(i) prohibit Eligible Subscribers from requesting the Issue of a Certificate anonymously or by means of a pseudonym; and

(ii) permit the DCA to Authenticate each Eligible Subscriber.

3.1.4 Rules for Interpreting Various Name Forms

(A) Provision in relation to name forms is made in Annex B.

3.1.5 Uniqueness of Names

(A) Provision in relation to the uniqueness of names is made in Annex B.

3.1.6 Recognition, Authentication, and Role of Trademarks

(A) Provision in relation to the use of trademarks, trade names and other restricted information in Certificates is made in Section L11 of the Code (Subscriber Obligations).

3.2 INITIAL IDENTITY VALIDATION

3.2.1 Method to Prove Possession of Private Key

(A) Provision is made in the SMKI RAPP in relation to:

(i) the procedure to be followed by an Eligible Subscriber in order to prove its possession of the Private Key which is associated with the Public Key to be contained in any Certificate that is the subject of a Certificate Signing Request; and

(ii) the procedure established for this purpose is in accordance with the procedure in PKCS#10.

3.2.2 Authentication of Organisation Identity

(A) Provision is made in the SMKI RAPP section 5.5 in relation to the:

(i) procedure to be followed by a Party in order to become an Authorised Subscriber;

(ii) criteria in accordance with which the DCA will determine whether a Party is entitled to become an Authorised Subscriber; and

(iii) requirement that the Party shall be Authenticated by the DCA for that purpose.

(B) Provision is made in the SMKI RAPP section 5 for the purpose of ensuring that the criteria in accordance with which the DCA shall Authenticate a Party shall be set to the level pursuant to the SMKI PMA Guidance on "Verifying Organisation Identity" published on the Website.

3.2.3 Authentication of Individual Identity

(A) Provision is made in the SMKI RAPP sections 5.2 and 5.3 in relation to the Authentication of persons engaged by Authorised Subscribers, which provides for all such persons to have their identity and authorisation verified to the level pursuant to the SMKI PMA Guidance on "Verifying Individual Identity" published on the Website.

3.2.4 Authentication of Devices

(A) Not used.

3.2.5 Non-verified Subscriber Information

(A) The DCA shall:

(i) verify all information in relation to DCA Certificates;

(ii) require each Eligible Subscriber to verify the information contained in any Certificate Signing Request in respect of a Device Certificate.

(B) Further provision on the content of DCA Certificates is made in Section L11 of the Code (Subscriber Obligations).

3.2.6 Validation of Authority

See Part 3.2.2 of this Policy.

3.2.7 Criteria for Interoperation

[*Not applicable in this Policy*]

3.3 IDENTIFICATION AND AUTHENTICATION FOR RE-KEY REQUESTS

3.3.1 Identification and Authentication for Routine Re-Key

(A) This Policy does not support Certificate Re-Key.

(B) The DCA shall not provide a Certificate Re-Key service.

3.3.2 Identification and Authentication for Re-Key after Revocation

[*Not applicable in this Policy*]

3.4 IDENTIFICATION AND AUTHENTICATION FOR REVOCATION REQUEST

[*Not applicable in this Policy*]

4 CERTIFICATE LIFE-CYCLE OPERATIONAL REQUIREMENTS

4.1 CERTIFICATE APPLICATION

4.1.1 Submission of Certificate Applications

(A) Provision is made in the SMKI RAPP in relation to:

(i) in respect of a Device Certificate:

(a) the circumstances in which an Eligible Subscriber may submit a Certificate Signing Request; and

(b) the means by which it may do so, including through the use of an authorised System.

4.1.2 Enrolment Process and Responsibilities

(A) Provision is made where applicable in the SMKI RAPP sections 5 and 6 in relation to the:

(i) establishment of an enrolment process in respect of organisations, individuals, Systems and Devices in order to Authenticate them and verify that they are authorised to act on behalf of an Eligible Subscriber or Authorised Subscriber in its capacity as such; and

(ii) maintenance by the DCA of a list of organisations, individuals, Systems and Devices enrolled in accordance with that process.

4.1.3 Enrolment Process for the Registration Authority and its Representatives

(A) Provision is made in the SMKI RAPP section 6 in relation to the establishment of an enrolment process in respect of DCA Personnel and DCA Systems:

(i) in order to Authenticate them and verify that they are authorised to act on behalf of the DCA in its capacity as the Registration Authority; and

(ii) including in particular, for that purpose, provision:

(a) for the face-to-face or video link Authentication of all SMKI Registration Authority Personnel by a SMKI Registration Authority Manager; and

(b) for all SMKI Registration Authority Personnel to have their identify and authorisation verified to the level pursuant to the SMKI PMA Guidance on “Verifying Individual Identity” published on the Website.

4.2 CERTIFICATE APPLICATION PROCESSING

4.2.1 Performing Identification and Authentication Functions

(A) Provision is made in the SMKI RAPP section 5 in relation to the Authentication by the DCA of Eligible Subscribers which submit a Certificate Signing Request.

4.2.2 Approval or Rejection of Certificate Applications

(A) Where any Certificate Signing Request fails to satisfy the requirements set out in the SMKI RAPP, the SMKI Interface Design Specification (SMKI IDS), this Policy or any other provision of the Code, the DCA:

(i) shall reject it and refuse to Issue the Certificate which was the subject of the Certificate Signing Request; and

(ii) shall give notice to the Party which made the Certificate Signing Request of the reasons for its rejection.

(B) Where any Certificate Signing Request satisfies the requirements set out in the SMKI RAPP, SMKI IDS, this Policy or any other provision of the Code, the DCA shall Issue the Certificate which was the subject of the Certificate Signing Request.

4.2.3 Time to Process Certificate Applications

(A) Provision in relation to the performance of the SMKI Services by the DCA is made in Section L8 of the Code (SMKI Performance Standards and

Demand Management).

4.3 CERTIFICATE ISSUANCE

4.3.1 DCA Actions during Certificate Issuance

(A) The DCA may Issue a Certificate only:

(i) in accordance with the provisions of this Policy, the SMKI RAPP and the SMKI IDS; and

(ii) in response to a Certificate Signing Request made by an Eligible Subscriber in accordance with the SMKI RAPP.

(B) The DCA shall ensure that:

(i) each DCA Certificate Issued by it contains information that it has verified to be correct and complete; and

(ii) each Device Certificate Issued by it contains information consistent with the information in the Certificate Signing Request.

(C) A DCA Certificate may only be:

(i) Issued by the DCA; and

(ii) for that purpose, signed using the Root DCA Private Key.

(D) A Device Certificate may only be:

(i) Issued by the DCA; and

(ii) for that purpose, signed using an Issuing DCA Private Key.

(E) The DCA shall not Issue a Device Certificate which is signed using an Issuing DCA Private Key after the first in time of the following:

(i) the time which is three months after the time at which any element of the Issuing DCA Private Key first became operational;

(ii) the time at which the DCA Issues the 100,000th Device Certificate which is signed using that Issuing DCA Private Key.

(F) For the purposes of paragraph (E), the DCA shall ensure that the Device CPS incorporates:

(i) a procedure for determining:

(a) how the DCA will calculate when each of the times specified in that paragraph occurs; and

(b) for that purpose, when any element of the Issuing DCA Private Key first became operational; and

(ii) provisions for notifying the SMKI PMA when either of the times specified in that paragraph is approaching.

(G) The DCA shall not issue a Certificate containing a Public Key where it is aware that the Public Key is the same as the Public Key contained in any other Certificate that was previously issued by it.

4.3.2 Notification to Eligible Subscriber by the DCA of Issuance of Certificate

(A) Provision is made in the SMKI IDS sections 2.3.1.9, 2.4.1.4 and 2.5.1.4for the DCA to notify an Eligible Subscriber where that Eligible Subscriber is Issued with a Certificate which was the subject of a Certificate Signing Request made by it.

4.4 CERTIFICATE ACCEPTANCE

4.4.1 Conduct Constituting Certificate Acceptance

(A) Provision is made in the SMKI IDS to:

(i) specify a means by which an Eligible Subscriber may clearly indicate to the DCA its rejection of a Certificate which has been Issued to it (SMKI IDS sections 2.3.1.10, 2.4.1.5 and 2.5.1.5); and

(ii) ensure that each Eligible Subscriber to which a Certificate has been Issued, and which has not rejected it, is treated as having accepted that

Certificate (SMKI IDS section 2.2).

(B) A Certificate which has been Issued by the DCA shall not be treated as valid for any purposes of this Policy or the Code until it is treated as having been accepted by the Eligible Subscriber to which it was Issued.

(C) The DCA shall maintain a record of all Certificates which have been Issued by it and are treated as accepted by a Subscriber.

(D) Further provision in relation to the rejection and acceptance of Certificates is made in Section L11.6 of the Code.

4.4.2 Publication of Certificates by the DCA

(A) Provision in relation to the publication of Certificates is made in Part 2 of this Policy.

4.4.3 Notification of Certificate Issuance by the DCA to Other Entities

(A) The DCA shall give notice of the Issue of a Certificate only to the Eligible Subscriber which submitted a Certificate Signing Request in respect of that Certificate (SMKI IDS sections 2.3.1.9, 2.4.1.4 and 2.5.1.4).

4.5 KEY PAIR AND CERTIFICATE USAGE

4.5.1 Subscriber Private Key and Certificate Usage

(A) Provision for restrictions on the use by Subscribers of Private Keys in respect of Certificates is made in:

(i) Section L11.8 of the Code; and

(ii) this Policy.

4.5.2 Relying Party Public Key and Certificate Usage

(A) Provision in relation to reliance that may be placed on a Certificate is made in Section L12 of the Code (Relying Party Obligations).

4.6 CERTIFICATE RENEWAL

4.6.1 Circumstances of Certificate Renewal

(A) This Policy does not support the renewal of Certificates.

(B) The DCA may only replace, and shall not renew, any Certificate.

4.6.2 Circumstances of Certificate Replacement

(A) Where the DCA Systems or any DCA Private Key is (or is suspected by the DCA of being) Compromised, the DCA shall:

(i) immediately notify the SMKI PMA;

(ii) provide the SMKI PMA with all of the information known to it in relation to the nature and circumstances of the event of Compromise or suspected Compromise; and

(iii) where the Compromise or suspected Compromise relates to a DCA Private Key:

(a) ensure that the Private Key is no longer used;

(b) promptly notify each of the Subscribers for any Device Certificates Issued using that Private Key; and

(c) promptly both notify the SMKI PMA and verifiably destroy the DCA Private Key Material.

(B) Where the Root DCA Private Key is Compromised (or is suspected by the DCA of being Compromised), the DCA:

(i) may issue a replacement for any DCA Certificate that has been Issued using that Private Key; and

(ii) shall ensure that the Subscriber for that DCA Certificate applies for the Issue of a new Certificate in accordance with this Policy.

(C) An Eligible Subscriber may request a replacement for a Certificate at any time by applying for the Issue of a new Device Certificate in accordance with this Policy.

4.6.3 Who May Request a Replacement Certificate

See Part 4.1 of this Policy.

4.6.4 Processing Replacement Certificate Requests

See Part 4.2 of this Policy

4.6.5 Notification of Replacement Certificate Issuance to a Subscriber

See Part 4.3.2 of this Policy.

4.6.6 Conduct Constituting Acceptance of a Replacement Certificate

See Part 4.4.1 of this Policy.

4.6.7 Publication of a Replacement Certificate by the DCA

See Part 4.4.2 of this Policy.

4.6.8 Notification of Certificate Issuance by the DCA to Other Entities

See Part 4.4.3 of this Policy

4.7 CERTIFICATE RE-KEY

4.7.1 Circumstances for Certificate Re-Key

(A) This Policy does not support Certificate Re-Key.

(B) The DCA shall not provide a Certificate Re-Key service.

(C) Where a new Key Pair has been generated by a Device, the Eligible Subscriber which is responsible for that Device shall apply for the Issue of a new Certificate in accordance with this Policy.

4.7.2 Who may Request Certification of a New Public Key

[*Not applicable in this Policy*]

4.7.3 Processing Certificate Re-Keying Requests

[*Not applicable in this Policy*]

4.7.4 Notification of New Certificate Issuance to Subscriber

[*Not applicable in this Policy*]

4.7.5 Conduct Constituting Acceptance of a Re-Keyed Certificate

[*Not applicable in this Policy*]

4.7.6 Publication of the Re-Keyed Certificate by the DCA

[*Not applicable in this Policy*]

4.7.7 Notification of Certificate Issuance by the DCA to Other Entities

[*Not applicable in this Policy*]

4.8 CERTIFICATE MODIFICATION

4.8.1 Circumstances for Certificate Modification

(A) This Policy does not support Certificate modification.

(B) Neither the DCA nor any Subscriber may modify a Certificate.

4.8.2 Who may request Certificate Modification

[*Not applicable in this Policy*]

4.8.3 Processing Certificate Modification Requests

[*Not applicable in this Policy*]

4.8.4 Notification of New Certificate Issuance to Subscriber

[*Not applicable in this Policy*]

4.8.5 Conduct Constituting Acceptance of Modified Certificate

[*Not applicable in this Policy*]

4.8.6 Publication of the Modified Certificate by the DCA

[*Not applicable in this Policy*]

4.8.7 Notification of Certificate Issuance by the DCA to Other Entities

[*Not applicable in this Policy*]

4.9 CERTIFICATE REVOCATION AND SUSPENSION

4.9.1 Circumstances for Revocation

(A) This Policy does not support the revocation or suspension of Certificates.

(B) The DCA shall not provide any service of revoking or suspending a Certificate.

4.9.2 Who can Request Revocation

[*Not applicable in this Policy*]

4.9.3 Procedure for Revocation Request

[*Not applicable in this Policy*]

4.9.4 Revocation Request Grace Period

[*Not applicable in this Policy*]

4.9.5 Time within which DCA must process the Revocation Request

[*Not applicable in this Policy*]

4.9.6 Revocation Checking Requirements for Relying Parties

[*Not applicable in this Policy*]

4.9.7 CRL Issuance Frequency (if applicable)

[*Not applicable in this Policy*]

4.9.8 Maximum Latency for CRLs (if applicable)

[*Not applicable in this Policy*]

4.9.9 On-line Revocation/Status Checking Availability

[*Not applicable in this Policy*]

4.9.10 On-line Revocation Checking Requirements

[*Not applicable in this Policy*]

4.9.11 Other Forms of Revocation Advertisements Available

[*Not applicable in this Policy*]

4.9.12 Special Requirements in the Event of Key Compromise

See Part 4.6.2 of this Policy.

4.9.13 Circumstances for Suspension

[*Not applicable in this Policy*]

4.9.14 Who can Request Suspension

[*Not applicable in this Policy*]

4.9.15 Procedure for Suspension Request

[*Not applicable in this Policy*]

4.9.16 Limits on Suspension Period

[*Not applicable in this Policy*]

4.10 CERTIFICATE STATUS SERVICES

4.10.1 Operational Characteristics

[*Not applicable in this Policy*]

4.10.2 Service Availability

[*Not applicable in this Policy*]

4.10.3 Optional Features

[*Not applicable in this Policy*]

4.11 END OF SUBSCRIPTION

[*Not applicable in this Policy*]

4.12 KEY ESCROW AND RECOVERY

4.12.1 Key Escrow and Recovery Policies and Practices

(A) This Policy does not support Key Escrow.

(B) The DCA shall not provide any Key Escrow service.

4.12.2 Session Key Encapsulation and Recovery Policy and Practices

[*Not applicable in this Policy*]

5 FACILITY, MANAGEMENT AND OPERATIONAL CONTROLS

5.1 PHYSICAL CONTROLS

5.1.1 Site Location and Construction

(A) The DCA shall ensure that the DCA Systems are operated in a sufficiently secure environment, which shall at least satisfy the requirements set out at Section G2 (System Security: Obligations on the DCC) and Section G5 (Information Security: Obligations on the DCC and Users) of the Code.

(B) The DCA shall ensure that:

(i) all of the physical locations in which the DCA Systems are situated, operated, routed or directly accessed are in the United Kingdom;

(ii) all bespoke Security Related Functionality is developed, specified, designed, built and tested only within the United Kingdom; and

(iii) all Security Related Functionality is integrated, configured, tested in situ, implemented, operated and maintained only within the United Kingdom.

(C) The DCA shall ensure that the DCA Systems cannot be indirectly accessed from any location outside the United Kingdom.

(D) The DCA shall ensure that the Device CPS incorporates provisions designed to ensure that all physical locations in which the manufacture of Certificates and Time-Stamping take place are at all times manually or electronically monitored for unauthorised intrusion in accordance with the SMKI PMA Guidance on “Protective Monitoring” published on the Website.

(E) The DCA shall ensure that the Device CPS incorporates provisions designed to ensure that all PINs, pass-phrases and passwords used for the purposes of carrying out the functions of the DCA are stored in secure containers accessible only to appropriately authorised individuals.

(F) The DCA shall ensure that the DCA Systems are Separated from any OCA

Systems, save that any Systems used for the purposes of the Registration Authority functions of the DCA and OCA shall not require to be Separated.

5.1.2 Physical Access

(A) The DCA shall ensure that the Device CPS incorporates provisions in relation to access control, including in particular provisions designed to:

(i) establish controls such that only appropriately authorised personnel may have unescorted physical access to DCA Systems or any System used for the purposes of Time-Stamping;

(ii) ensure that any unauthorised personnel may have physical access to such Systems only if appropriately authorised and supervised;

(iii) ensure that a site access log is both maintained and periodically inspected for all locations at which such Systems are sited; and

(iv) ensure that all removable media which contain sensitive plain text Data and are kept at such locations are stored in secure containers accessible only to appropriately authorised individuals.

5.1.3 Power and Air Conditioning

(A) The DCA shall ensure that the Device CPS incorporates provisions in relation to power and air conditioning at all physical locations in which the DCA Systems are situated.

5.1.4 Water Exposure

(A) The DCA shall ensure that the Device CPS incorporates provisions in relation to water exposure at all physical locations in which the DCA Systems are situated.

5.1.5 Fire Prevention and Protection

(A) The DCA shall ensure that the Device CPS incorporates provisions in relation to fire prevention and protection at all physical locations in which the DCA

Systems are situated.

5.1.6 Media Storage

(A) The DCA shall ensure that the Device CPS incorporates provisions designed to ensure that appropriate controls are placed on all media used for the storage of Data held by it for the purposes of carrying out its functions as the DCA.

5.1.7 Waste Disposal

(A) The DCA shall ensure that all media used to store Data held by it for the purposes of carrying out its functions as the DCA are disposed of only using secure methods of disposal in accordance with https://www.ncsc.gov.uk/guidance/secure-sanitisation-storage-media.

5.1.8 Off-Site Back-Up

(A) The DCA shall regularly carry out a Back-Up of:

(i) all Data held on the DCA Systems which are critical to the operation of those Systems or continuity in the provision of the SMKI Services; and

(ii) all other sensitive Data.

(B) For the purposes of paragraph (A), the DCA shall ensure that the Device CPS incorporates provisions which identify the categories of critical and sensitive Data that are to be Backed-Up.

(C) The DCA shall ensure that Data which are Backed-Up in accordance with paragraph (A):

(i) are stored on media that are located in physically secure facilities in different locations to the sites at which the Data being Backed-Up are ordinarily held;

(ii) are protected in accordance with the outcome of a risk assessment which is documented in the Device CPS, including when being transmitted for the purposes of Back-Up; and

(iii) to the extent to which they comprise DCA Private Key Material, are Backed-Up:

(a) using the proprietary Back-Up mechanisms specific to the relevant Cryptographic Module; and

(b) in a manner that is compliant with FIPS 140-2 Level 3 (or any equivalent to that Federal Information Processing Standard which updates or replaces it from time to time).

(D) The DCA shall ensure that, where any elements of the DCA Systems, any Data held for the purposes of providing the SMKI Services, or any items of DCA equipment are removed from their primary location, they continue to be protected in accordance with the security standard appropriate to the primary location.

5.2 PROCEDURAL CONTROLS

5.2.1 Trusted Roles

(A) The DCA shall ensure that:

(i) no individual may carry out any activity which involves access to resources, or Data held on, the DCA Systems unless that individual has been expressly authorised to have such access;

(ii) each member of DCA Personnel has a clearly defined level of access to the DCA Systems and the premises in which they are located;

(iii) no individual member of DCA Personnel is capable, by acting alone, of engaging in any action by means of which the DCA Systems may be Compromised to a material extent; and

(iv) the Device CPS incorporates provisions designed to ensure that appropriate controls are in place for the purposes of compliance by the DCA with the requirements of this paragraph.

5.2.2 Number of Persons Required per Task

(A) The DCA shall ensure that the Device CPS incorporates provisions designed to establish:

(i) the appropriate separation of roles between the different members of DCA Personnel; and

(ii) the application of controls to the actions of all members of DCA Personnel who are Privileged Persons, identifying in particular any controls designed to ensure that the involvement of more than one individual is required for the performance of certain functions.

(B) The DCA shall ensure that the Device CPS, as a minimum, makes provision for the purposes of paragraph (A) in relation to the following roles:

(i) DCA Systems administration;

(ii) DCA Systems operations;

(iii) DCA Systems security; and

(iv) DCA Systems auditing.

5.2.3 Identification and Authentication for Each Role

See Part 5.2.2 of this Policy.

5.2.4 Roles Requiring Separation of Duties

See Part 5.2.2 of this Policy.

5.3 PERSONNEL CONTROLS

5.3.1 Qualification, Experience and Clearance Requirements

(A) The DCA shall ensure that all DCA Personnel must:

(i) be appointed to their roles in writing;

(ii) be bound by contract to the terms and conditions relevant to their roles;

(iii) have received appropriate training with respect to their duties;

(iv) be bound by contract not to disclose any confidential, sensitive, personal or security-related Data except to the extent necessary for the performance of their duties or for the purposes of complying with any requirement of law; and

(v) in so far as can reasonably be ascertained by the DCA, not have been previously relieved of any past assignment (whether for the DCA or any other person) on the grounds of negligence or any other failure to perform a duty.

(B) The DCA shall ensure that all DCA Personnel have, as a minimum, passed a Security Check before commencing their roles.

5.3.2 Background Check Procedures

See Part 5.3.1 of this Policy.

5.3.3 Training Requirements

See Part 5.3.1 of this Policy.

5.3.4 Retraining Frequency and Requirements

(A) The DCA shall ensure that the Device CPS incorporates appropriate provisions relating to the frequency and content of retraining and refresher training to be undertaken by members of DCA Personnel.

5.3.5 Job Rotation Frequency and Sequence

(A) The DCA shall ensure that the Device CPS incorporates appropriate provisions relating to the frequency and sequence of job rotations to be undertaken by members of DCA Personnel.

5.3.6 Sanctions for Unauthorised Actions

(A) The DCA shall ensure that the Device CPS incorporates appropriate provisions relating to sanctions for unauthorised actions undertaken by members of DCA Personnel.

5.3.7 Independent Contractor Requirements

(A) In accordance with the provisions of the Code, references to the DCA in this Policy include references to persons with whom the DCA contracts in order to secure performance of its obligations as the DCA.

5.3.8 Documentation Supplied to Personnel

(A) The DCA shall ensure that all DCA Personnel are provided with access to all documents relevant to their roles or necessary for the performance of their duties, including in particular:

(i) this Policy;

(ii) the Device CPS; and

(iii) any supporting documentation, statutes, policies or contracts.

5.4 AUDIT LOGGING PROCEDURES

5.4.1 Types of Events Recorded

(A) The DCA shall ensure that:

(i) the DCA Systems record all systems activity in an audit log;

(ii) the Device CPS incorporates a comprehensive list of all events that are to be recorded in an audit log in relation to:

(a) the activities of DCA Personnel;

(b) the use of DCA equipment;

(c) the use of (including both authorised and unauthorised access, and attempted access to) any premises at which functions of the DCA are carried out;

(d) communications and activities that are related to the Issue of

Certificates (in so far as not captured by the DCA Systems audit log); and

(iii) it records in an audit log all the events specified in paragraph (ii).

5.4.2 Frequency of Processing Log

(A) The DCA shall ensure that:

(i) the audit logging functionality in the DCA Systems is fully enabled at all times;

(ii) all DCA Systems activity recorded in the Audit Log is recorded in a standard format that is compliant with:

(a) British Standard BS 10008:2014 (Evidential Weight and Legal Admissibility of Electronic Information); or

(b) any equivalent to that British Standard which updates or replaces it from time to time; and

(iii) it monitors the DCA Systems in compliance with the SMKI PMA Guidance on “Protective Monitoring” published on the Website.

(B) The DCA shall ensure that the Device CPS incorporates provisions which specify:

(i) how regularly information recorded in the Audit Log is to be reviewed; and

(ii) what actions are to be taken by it in response to types of events recorded in the Audit Log.

(C) The DCA shall ensure that the Device CPS incorporates provisions in relation to access to the Audit Log, providing in particular that:

(i) Data contained in the Audit Log must not be accessible other than on a read-only basis; and

(ii) access to those Data must be limited to those members of DCA Personnel who are performing a dedicated system audit role.

5.4.3 Retention Period for Audit Log

(A) The DCA shall:

(i) retain the Audit Log so that it incorporates, on any given date, a record of all system events occurring during a period of at least twelve months prior to that date; and

(ii) ensure that a copy of the Audit Log incorporating a record of all system events occurring prior to the beginning of that period is archived in accordance with the requirements of Part 5.5 of this Policy.

5.4.4 Protection of Audit Log

(A) The DCA shall ensure that:

(i) to the extent to which the Audit Log is retained electronically, the Data stored in it cannot be accessed other than on a read-only basis, and are protected from unauthorised viewing, modification and deletion in accordance with:

(a) British Standard BS 10008:2014 (Evidential Weight and Legal Admissibility of Electronic Information); or

(b) any equivalent to that British Standard which updates or replaces it from time to time; and

(ii) to the extent to which the Audit Log is retained in non-electronic form, the Data stored in it are appropriately protected from unauthorised viewing, modification and destruction in order to ensure that their integrity is maintained for evidential purposes.

5.4.5 Audit Log Back-Up Procedures

(A) The DCA shall ensure that the Data contained in the Audit Log are Backed-

Up (or, to the extent that the Audit Log is retained in non-electronic form, are copied):

(i) on a daily basis; or

(ii) if activity has taken place on the DCA Systems only infrequently, in accordance with the schedule for the regular Back-Up of the Data held on those Systems.

(B) The DCA shall ensure that all Data contained in the Audit Log which are Backed-Up are, during Back-Up:

(i) held in accordance with the outcome of a risk assessment which is documented in the Device CPS; and

(ii) protected to the same standard of protection as the primary copy of the Audit Log in accordance with Part 5.4.4 of this Policy.

5.4.6 Audit Collection System (Internal or External)

(A) The DCA shall ensure that the Device CPS incorporates provisions in relation to its system for collecting Data for the purpose of populating the Audit Log.

5.4.7 Notification to Event-Causing Subject

(A) The DCA shall ensure that the Device CPS incorporates provisions in relation to its notification of any person who is (or is responsible for any System which is) the direct cause of an event recorded in the Audit Log.

5.4.8 Vulnerability Assessments

(A) Provision is made in Sections G2.13 to G2.14 of the Code (Management of Vulnerabilities) in relation to the carrying out of vulnerability assessments in respect of the DCA Systems.

5.5 RECORDS ARCHIVAL

5.5.1 Types of Records Archived

(A) The DCA shall ensure that it archives:

(i) the Audit Log in accordance with Part 5.4.3 of this Policy;

(ii) its records of all Data submitted to it by Eligible Subscribers for the purposes of Certificate Signing Requests; and

(iii) any other Data specified in this Policy or the Code as requiring to be archived in accordance with this Part 5.5.

5.5.2 Retention Period for Archive

(A) The DCA shall ensure that all Data which are Archived are retained for a period of at least seven years from the date on which they were Archived.

5.5.3 Protection of Archive

(A) The DCA shall ensure that Data held in its Archive are:

(i) protected against any unauthorised access;

(ii) adequately protected against environmental threats such as temperature, humidity and magnetism; and

(iii) incapable of being modified or deleted.

5.5.4 Archive Back-Up Procedures

(A) The DCA shall ensure that the Device CPS incorporates provisions in relation to its procedures for the Back-Up of its Archive.

5.5.5 Requirements for Time-Stamping of Records

(A) Provision in relation to Time-Stamping is made in Part 6.8 of this Policy.

5.5.6 Archive Collection System (Internal or External)

(A) The DCA shall ensure that the Device CPS incorporates provisions in relation to its system for collecting Data for the purpose of populating the Archive.

5.5.7 Procedures to Obtain and Verify Archive Information

(A) The DCA shall ensure that:

(i) Data held in the Archive are stored in a readable format during their retention period; and

(ii) those Data remains accessible at all times during their retention period, including during any period of interruption, suspension or cessation of the DCA's operations.

(B) The DCA shall ensure that the Device CPS incorporates provisions in relation to the periodic verification by the DCA of the Data held in the Archive.

5.6 KEY CHANGEOVER

5.6.1 Device Certificate Key Changeover

(A) The DCA shall Issue a new Device Certificate in relation to a Device where a new Certificate Signing Request is submitted by an Eligible Subscriber in accordance with the requirements of the SMKI IDS sections 2.3.1.6 to 2.3.1.10, 2.4.1.1 to 2.4.1.5 and 2.5.1.1 to 2.5.1.4and this Policy.

5.6.2 DCA Key Changeover

(A) Where the DCA ceases to use an Issuing DCA Private Key in accordance with the requirements of Part 4.3.1(E) of this Policy, it shall:

(i) verifiably destroy the Issuing DCA Private Key Material;

(ii) not revoke the related Issuing DCA Certificate (which may continue to be used for the purpose of validating Digital Signatures generated using the Issuing DCA Private Key);

(iii) generate a new Key Pair;

(iv) ensure that any Device Certificate subsequently Issued by it is Issued using the Issuing DCA Private Key from the newly-generated Key Pair:

(a) until the time determined in accordance with Part 4.3.1(E) of this Policy; and

(b) subject to the provisions of Part 5.7.1(C) of this Policy; and

(v) in its capacity as the Root DCA:

(a) Issue a new Issuing DCA Certificate; and

(b) promptly lodge that Issuing DCA Certificate in the SMKI Repository.

(B) The DCA shall ensure that the actions taken by it in accordance with the requirements of paragraph (A) are managed so as to prevent any disruption to the provision of the SMKI Services.

5.7 COMPROMISE AND DISASTER RECOVERY

5.7.1 Incident and Compromise Handling Procedures

(A) The DCA shall ensure that the Device CPS incorporates a business continuity plan which shall be designed to ensure continuity in, or (where there has been unavoidable discontinuity) the recovery of, the provision of the SMKI Services in the event of any Compromise of the DCA Systems or major failure in the DCA processes.

(B) The DCA shall ensure that the procedures set out in the business continuity plan are:

(i) compliant with ISO 22301 and ISO 27031 (or any equivalent to those standards which update or replace them from time to time); and

(ii) tested periodically, and in any event at least once in each year, in order to ensure that they are operationally effective.

(C) In the event of the Compromise of any DCA Private Key, the DCA shall:

(i) not revoke the related Issuing DCA Certificate;

(ii) not revoke any Device Certificates Issued using the Issuing DCA Private Key;

(iii) not issue any further Device Certificates using the Issuing DCA Private Key;

(iv) treat the event in the same manner as if it were a Major Security Incident in accordance with Section G2 of the Code (System Security: Obligations on the DCC); and

(v) immediately notify the SMKI PMA.

(D) The DCA shall ensure that the Device CPS incorporates provisions setting out the approach to be taken by it in circumstances in which it suspects (or has reason to suspect) that any Issuing DCA Private Key or any part of the DCA Systems is Compromised.

5.7.2 Computing Resources, Software and/or Data are Corrupted

(A) The DCA shall ensure that the business continuity plan established in accordance with Part 5.7.1 of this Policy incorporates provisions setting out the steps to be taken in the event of any loss of or corruption to computing resources, software or Data.

5.7.3 Entity Private Key Compromise Procedures

See Part 5.7.1 of this Policy.

5.7.4 Business Continuity Capabilities after a Disaster

(A) The DCA shall ensure that the business continuity plan established in accordance with Part 5.7.1 of this Policy is designed to ensure the recovery of the provision of the SMKI Services within not more than 12 hours of the occurrence of any event causing discontinuity.

5.8 CERTIFICATION AUTHORITY AND REGISTRATION AUTHORITY TERMINATION

[*Not applicable in this Policy*]

6 <u>TECHNICAL SECURITY CONTROLS</u>

The DCA shall ensure that the Device CPS incorporates detailed provision in relation to the technical controls to be established and operated for the purposes of the exercise of its functions as the Root DCA, the Issuing DCA and the Registration Authority.

6.1 KEY PAIR GENERATION AND INSTALLATION

6.1.1 Key Pair Generation

(A) The DCA shall ensure that all Key Pairs which it uses for the purposes of this Policy are generated:

(i) in a protected environment compliant with FIPS 140-2 Level 3 (or any equivalent to that Federal Information Processing Standard which updates or replaces it from time to time);

(ii) using multi-person control, such that no single Privileged Person is capable of generating any DCA Key; and

(iii) using random numbers which are such as to make it computationally infeasible to regenerate those Key Pairs even with knowledge of when and by means of what equipment they were generated.

(B) The DCA shall not generate any Private Key or Public Key other than a DCA Key.

6.1.2 Private Key Delivery to Subscriber

(A) In accordance with Part 6.1.1(B), the DCA shall not generate any Private Key for delivery to a Subscriber.

6.1.3 Public Key Delivery to Certificate Issuer

(A) The DCA shall ensure that the Device CPS incorporates provisions:

(i) in relation to the mechanism by which Public Keys of Subscribers are delivered to it for the purpose of the exercise of its functions as the Root DCA and Issuing DCA; and

(ii) ensuring that the mechanism uses a recognised standard protocol such as PKCS#10.

6.1.4 DCA Public Key Delivery to Relying Parties

(A) The DCA shall ensure that the Device CPS incorporates provisions:

(i) in relation to the manner by which each DCA Public Key is to be lodged in the SMKI Repository; and

(ii) designed to ensure that the DCA Public Keys are securely lodged in the SMKI Repository in such a manner as to guarantee that their integrity is maintained.

6.1.5 Key Sizes

(A) The DCA and every Subscriber shall ensure that all Private Keys and Public Keys which each of them may use for the purposes of this Policy are of the size and characteristics set out in the GB Companion Specification.

6.1.6 Public Key Parameters Generation and Quality Checking

(A) The DCA shall ensure that any Public Key used by it for the purposes of this Policy shall be of values and lengths that make the success of known attacks infeasible.

(B) Each Subscriber shall ensure that any Public Key used by it for the purposes of this Policy shall be of values and lengths that make the success of known attacks infeasible.

6.1.7 Key Usage Purposes (as per X.509 v3 `keyUsage` Field)

(A) The DCA shall ensure that each Certificate that is Issued by it has a `keyUsage` field in accordance with RFC5759 and RFC5280.

(B) The DCA shall ensure that each Device Certificate that is Issued by it has a `keyUsage` of either:

(i) `digitalSignature`; or

(ii) `keyAgreement`.

(C) The DCA shall ensure that each DCA Certificate that is Issued by it has a `keyUsage` of `keyCertSign`.

(D) The DCA shall ensure that no `keyUsage` values may be set in a Device Certificate or DCA Certificate other than in accordance with this Part 6.1.7.

6.2 PRIVATE KEY PROTECTION AND CRYPTOGRAPHIC MODULE ENGINEERING CONTROLS

6.2.1 Cryptographic Module Standards and Controls

(A) The DCA shall ensure that all DCA Private Keys shall be:

(i) protected to a high standard of assurance by physical and logical security controls; and

(ii) stored in and operated from within a Cryptographic Module which is compliant with FIPS 140-2 Level 3 (or any equivalent to that Federal Information Processing Standard which updates or replaces it from time to time).

(B) The DCA shall ensure that all DCA Private Keys shall, where they affect the outcome of any Certificates Issued by it, be protected by, stored in and operated from within a Cryptographic Module which is compliant with FIPS 140-2 Level 3 (or any equivalent to that Federal Information Processing Standard which updates or replaces it from time to time).

(C) The DCA shall ensure that no DCA Private Key shall be made available in either complete or unencrypted form except in a Cryptographic Module which is compliant with FIPS 140-2 Level 3 (or any equivalent to that Federal Information Processing Standard which updates or replaces it from time to time).

(D) The DCA shall ensure that any Cryptographic Module which is used for any purpose related to Certificate life-cycle management shall:

(i) operate so as to block access to itself following a number of failed consecutive attempts to access it using Activation Data, where that number shall be set out in the Device CPS; and

(ii) be required to be unblocked by an authorised member of DCA Personnel who has been Authenticated as such following a process which shall be set out in the Device CPS.

6.2.2 Private Key (m out of n) Multi-Person Control

See Part 6.1.1 of this Policy.

6.2.3 Private Key Escrow

(A) This Policy does not support Key Escrow.

(B) The DCA shall not provide any Key Escrow service.

6.2.4 Private Key Back-Up

(A) The DCA may Back-Up DCA Private Keys insofar as:

(i) each Private Key is protected to a standard which is at least equivalent to that required in relation to the principal Private Key in accordance with this Policy; and

(ii) where more than one Private Key is Backed-Up within a single security environment, each of the Private Keys which is Backed-Up within that environment must be protected to a standard which is at least equivalent to that required in relation to an Issuing DCA Private Key in accordance with this Policy.

6.2.5 Private Key Archival

(A) The DCA shall ensure that no DCA Key which is a Private Key is archived.

6.2.6 Private Key Transfer into or from a Cryptographic Module

(A) The DCA shall ensure that no DCA Private Key is transferred or copied other than:

(i) for the purposes of:

(a) Back-Up; or

(b) establishing an appropriate degree of resilience in relation to the provision of the SMKI Services;

(ii) in accordance with a level of protection which is compliant with FIPS 140-2 Level 3 (or any equivalent to that Federal Information Processing Standard which updates or replaces it from time to time).

6.2.7 Private Key Storage on Cryptographic Module

See Part 6.2.1 of this Policy.

6.2.8 Method of Activating Private Key

(A) The DCA shall ensure that the Cryptographic Module in which any DCA Private Key is stored may be accessed only by an authorised member of DCA Personnel who has been Authenticated following an Authentication process which:

(i) has an appropriate level of strength to ensure the protection of the Private Key; and

(ii) involves the use of Activation Data.

6.2.9 Method of Deactivating Private Key

(A) The DCA shall ensure that any DCA Private Key shall be capable of being de-activated by means of the DCA Systems, at least by:

(i) the actions of:

(a) turning off the power;

(b) logging off;

(c) carrying out a system reset; and

(ii) a period of inactivity of a length which shall be set out in the Device CPS.

6.2.10 Method of Destroying Private Key

(A) The DCA shall ensure that the Device CPS incorporates provisions for the exercise of strict controls in relation to the destruction of DCA Keys.

(B) The DCA shall ensure that no DCA Key (whether in active use, existing as a copy for the purposes of resilience, or Backed-Up) is destroyed except in accordance with a positive decision by the DCA to destroy it.

6.2.11 Cryptographic Module Rating

See Part 6.2.1 of this Policy.

6.3 OTHER ASPECTS OF KEY PAIR MANAGEMENT

6.3.1 Public Key Archival

(A) The DCA shall ensure that it archives DCA Public Keys in accordance with the requirements of Part 5.5 of this Policy.

6.3.2 Certificate Operational Periods and Key Pair Usage Periods

(A) The DCA shall ensure that:

(i) the Validity Period of each Certificate shall be an indefinite period; and

(ii) for this purpose, it uses the `notAfter` value specified in Annex B.

6.4 ACTIVATION DATA

6.4.1 Activation Data Generation and Installation

(A) The DCA shall ensure that any Cryptographic Module within which a DCA Key is held has Activation Data that are unique and unpredictable.

(B) The DCA shall ensure that:

(i) these Activation Data, in conjunction with any other access control, shall be of an appropriate level of strength for the purposes of protecting the DCA Keys; and

(ii) where the Activation Data comprise any PINs, passwords or pass-phrases, the DCA shall have the ability to change these at any time.

6.4.2 Activation Data Protection

(A) The DCA shall ensure that the Device CPS incorporates provision for the use of such cryptographic protections and access controls as are appropriate to protect against the unauthorised use of Activation Data.

6.4.3 Other Aspects of Activation Data

[*Not applicable in this Policy*]

6.5 COMPUTER SECURITY CONTROLS

6.5.1 Specific Computer Security Technical Requirements

(A) The DCA shall ensure that the Device CPS incorporates provisions in relation to the identification and implementation, following the conclusion of any threat assessment, of security measures which make provision for at least the following:

(i) the establishment of access controls in relation to the activities of the DCA;

(ii) the appropriate allocation of responsibilities to Privileged Persons;

(iii) the identification and Authentication of organisations, individuals and Systems involved in DCA activities;

(iv) the use of cryptography for communication and the protection of Data stored on the DCA Systems;

(v) the audit of security related events; and

(vi) the use of recovery mechanisms for DCA Keys.

6.5.2 Computer Security Rating

(A) The DCA shall ensure that the Device CPS incorporates provisions relating to the appropriate security rating of the DCA Systems.

6.6 LIFE-CYCLE TECHNICAL CONTROLS

6.6.1 System Development Controls

(A) The DCA shall ensure that any software which is developed for the purpose of establishing a functionality of the DCA Systems shall:

(i) take place in a controlled environment that is sufficient to protect against the insertion into the software of malicious code;

(ii) be undertaken by a developer which has a quality system that is:

(a) compliant with recognised international standards (such as ISO 9001:2000 or an equivalent standard); or

(b) available for inspection and approval by the SMKI PMA, and has been so inspected and approved.

6.6.2 Security Management Controls

(A) The DCA shall ensure that the Device CPS incorporates provisions which are designed to ensure that the DCA Systems satisfy the requirements of Section G2 (System Security: Obligations on the DCC) and Section G5 (Information Security: Obligations on the DCC and Users) of the Code.

6.6.3 Life-Cycle Security Controls

See Part 6.6.2 of this Policy.

6.7 NETWORK SECURITY CONTROLS

6.7.1 Use of Offline Root DCA

(A) The DCA shall ensure that its functions as the Root DCA are carried out on a part of the DCA Systems that is neither directly nor indirectly connected to any System which is not a part of the DCA Systems.

6.7.2 Protection Against Attack

(A) The DCA shall use its best endeavours to ensure that the DCA Systems are not Compromised, and in particular for this purpose that they are designed and operated so as to detect and prevent:

(i) any Denial of Service Event; and

(ii) any unauthorised attempt to connect to them.

(B) The DCA shall take reasonable steps to ensure that the DCA Systems cause or permit to be open at any time only those network ports, and allow only those protocols, which are required at that time for the effective operation of those Systems, and block all network ports and protocols which are not so required.

6.7.3 Separation of Issuing DCA

(A) The DCC shall ensure that, where its functions as the Issuing DCA are carried out on a part of the DCA Systems that is connected to an external network, they are carried out on a System that is Separated from all other DCA Systems.

6.7.4 Health Check of DCA Systems

(A) The DCA shall ensure that, in relation to the DCA Systems, a vulnerability assessment in accordance with Sections G2.13 – G2.15 of the Code (Management of Vulnerabilities) is carried out with such frequency as may be specified from time to time by the Independent SMKI Assurance Service Provider.

6.8 TIME-STAMPING

6.8.1 Use of Time-Stamping

(A) The DCA shall ensure that Time-Stamping takes place in relation to all Certificates and all other DCA activities which require an accurate record of time.

(B) The DCA shall ensure that the Device CA incorporates provisions in relation to the time source and mechanisms used by any Time-Stamping Authority which carries out Time-Stamping on behalf of the DCA.

7 CERTIFICATE, CRL AND OCSP PROFILES

7.1 CERTIFICATE PROFILES

(A) The DCA shall use only the Certificate Profiles in Annex B.

7.1.1 Version Number(s)

[*Not applicable in this Policy*]

7.1.2 Certificate Extensions

[*Not applicable in this Policy*]

7.1.3 Algorithm Object Identifiers

[*Not applicable in this Policy*]

7.1.4 Name Forms

[*Not applicable in this Policy*]

7.1.5 Name Constraints

[*Not applicable in this Policy*]

7.1.6 Certificate Policy Object Identifier

[*Not applicable in this Policy*]

7.1.7 Usage of Policy Constraints Extension

[*Not applicable in this Policy*]

7.1.8 Policy Qualifiers Syntax and Semantics

[*Not applicable in this Policy*]

7.1.9 Processing Semantics for the Critical Certificate Policies Extension

[*Not applicable in this Policy*]

7.2 CRL PROFILE

7.2.1 Version Number(s)

[*Not applicable in this Policy*]

7.2.2 CRL and CRL Entry Extensions

[*Not applicable in this Policy*]

7.3 OCSP PROFILE

7.3.1 Version Number(s)

[*Not applicable in this Policy*]

7.3.2 OCSP Extensions

[*Not applicable in this Policy*]

8 COMPLIANCE AUDIT AND OTHER ASSESSMENTS

8.1 FREQUENCY OR CIRCUMSTANCES OF ASSESSMENT

(A) Provision in relation to this is made in Appendix C of the Code (SMKI Compliance Policy).

8.2 IDENTITY/QUALIFICATIONS OF ASSESSOR

(A) Provision in relation to this is made in Appendix C of the Code (SMKI Compliance Policy).

8.3 ASSESSOR'S RELATIONSHIP TO ASSESSED ENTITY

(A) Provision in relation to this is made in Appendix C of the Code (SMKI Compliance Policy).

8.4 TOPICS COVERED BY ASSESSMENT

(A) Provision in relation to this is made in Appendix C of the Code (SMKI Compliance Policy).

8.5 ACTIONS TAKEN AS A RESULT OF DEFICIENCY

(A) Provision in relation to this is made in Appendix C of the Code (SMKI Compliance Policy).

8.6 COMMUNICATION OF RESULTS

(A) Provision in relation to this is made in Appendix C of the Code (SMKI Compliance Policy).

9 OTHER BUSINESS AND LEGAL MATTERS

In so far as provision is made in relation to all the matters referred to in this Part, it is found in the DCC Licence and the provisions of the Code (including in Section L11 (Subscriber Obligations) and Section L12 (Relying Party Obligations) of the Code).

9.1 FEES

(A) See the statement at the beginning of this Part.

9.1.1 Certificate Issuance or Renewal Fees

(A) See the statement at the beginning of this Part.

9.1.2 Device Certificate Access Fees

(A) See the statement at the beginning of this Part.

9.1.3 Revocation or Status Information Access Fees

(A) See the statement at the beginning of this Part.

9.1.4 Fees for Other Services

(A) See the statement at the beginning of this Part.

9.1.5 Refund Policy

(A) See the statement at the beginning of this Part.

9.2 FINANCIAL RESPONSIBILITY

9.2.1 Insurance Coverage

(A) See the statement at the beginning of this Part.

9.2.2 Other Assets

(A) See the statement at the beginning of this Part.

9.2.3 Insurance or Warranty Coverage for Subscribers and Subjects

(A) See the statement at the beginning of this Part.

9.3 CONFIDENTIALITY OF BUSINESS INFORMATION

9.3.1 Scope of Confidential Information

(A) See the statement at the beginning of this Part.

9.3.2 Information not within the Scope of Confidential Information

(A) See the statement at the beginning of this Part.

9.3.3 Responsibility to Protect Confidential Information

(A) See the statement at the beginning of this Part.

9.4 PRIVACY OF PERSONAL INFORMATION

9.4.1 Privacy Plan

(A) See the statement at the beginning of this Part.

9.4.2 Information Treated as Private

(A) See the statement at the beginning of this Part.

9.4.3 Information not Deemed Private

(A) See the statement at the beginning of this Part.

9.4.4 Responsibility to Protect Private Information

(A) See the statement at the beginning of this Part.

9.4.5 Notice and Consent to Use Private Information

(A) See the statement at the beginning of this Part.

9.4.6 Disclosure Pursuant to Judicial or Administrative Process

(A) See the statement at the beginning of this Part.

9.4.7 Other Information Disclosure Circumstances

(A) See the statement at the beginning of this Part.

9.5 INTELLECTUAL PROPERTY RIGHTS

(A) See the statement at the beginning of this Part.

9.6 REPRESENTATIONS AND WARRANTIES

9.6.1 Certification Authority Representations and Warranties

(A) See the statement at the beginning of this Part.

9.6.2 Registration Authority Representations and Warranties

(A) See the statement at the beginning of this Part.

9.6.3 Subscriber Representations and Warranties

(A) See the statement at the beginning of this Part.

9.6.4 Relying Party Representations and Warranties

(A) See the statement at the beginning of this Part.

9.6.5 Representations and Warranties of Other Participants

(A) See the statement at the beginning of this Part.

9.7 DISCLAIMERS OF WARRANTIES

(A) See the statement at the beginning of this Part.

9.8 LIMITATIONS OF LIABILITY

(A) See the statement at the beginning of this Part.

9.9 INDEMNITIES

(A) See the statement at the beginning of this Part.

9.10 TERM AND TERMINATION

9.10.1 Term

(A) See the statement at the beginning of this Part.

9.10.2 Termination of Device Certificate Policy

(A) See the statement at the beginning of this Part.

9.10.3 Effect of Termination and Survival

(A) See the statement at the beginning of this Part.

9.11 INDIVIDUAL NOTICES AND COMMUNICATIONS WITH PARTICIPANTS

9.11.1 Subscribers

(A) See the statement at the beginning of this Part.

9.11.2 Device Certification Authority

(A) See the statement at the beginning of this Part.

9.11.3 Notification

(A) See the statement at the beginning of this Part.

9.12 AMENDMENTS

9.12.1 Procedure for Amendment

(A) See the statement at the beginning of this Part.

9.12.2 Notification Mechanism and Period

(A) See the statement at the beginning of this Part.

9.12.3 Circumstances under which OID Must be Changed

(A) See the statement at the beginning of this Part.

9.13 DISPUTE RESOLUTION PROVISIONS

(A) See the statement at the beginning of this Part.

9.14 GOVERNING LAW

(A) See the statement at the beginning of this Part.

9.15 COMPLIANCE WITH APPLICABLE LAW

(A) See the statement at the beginning of this Part.

9.16 MISCELLANEOUS PROVISIONS

9.16.1 Entire Agreement

(A) See the statement at the beginning of this Part.

9.16.2 Assignment

(A) See the statement at the beginning of this Part.

9.16.3 Severability

(A) See the statement at the beginning of this Part.

9.16.4 Enforcement (Attorney's Fees and Waiver of Rights)

(A) `See the statement at the beginning of this Part.

9.16.5 Force Majeure

(A) See the statement at the beginning of this Part.

9.17 OTHER PROVISIONS

9.17.1 Device Certificate Policy Content

(A) See the statement at the beginning of this Part.

9.17.2 Third Party Rights

(A) See the statement at the beginning of this Part.

Annex A: Definitions and Interpretation

In this Policy, except where the context otherwise requires -

- expressions defined in Section A of the Code (Definitions and Interpretation) have the same meaning as is set out in that Section,
- the expressions in the left hand column below shall have the meanings given to them in the right hand column below,
- where any expression is defined in Section A of the Code (Definitions and Interpretation) and in this Annex, the definition in this Annex shall take precedence for the purposes of the Policy,
- the rule of interpretation set out at Part 1.1 of this Policy shall apply.

Activation Data

means any private Data (such as a password or the Data on a smartcard) which are used to access a Cryptographic Module.

Archive

means the archive of Data created in accordance with Part 5.5.1 of this Policy (and “**Archives**” and “**Archived**” shall be interpreted accordingly).

Audit Log

means the audit log created in accordance with Part 5.4.1 of this Policy.

Authentication

means the process of establishing that an individual, organisation, System or Device is what he or it claims to be (and “**Authenticate**” shall be interpreted accordingly).

Authorised Subscriber

means a Party or RDP which has successfully completed the procedures set out in the SMKI RAPP and has been authorised by the DCA to submit a Certificate Signing Request.

Certificate means either a Device Certificate or a DCA Certificate.

Certificate Profile means a table bearing that title in Annex B and specifying certain parameters to be contained within a Certificate.

Certificate Re-Key means a change to the Public Key contained within a Certificate bearing a particular serial number.

Certificate Signing Request means a request for a Certificate submitted by an Eligible Subscriber in accordance with the SMKI RAPP.

DCA Key means any Private Key or a Public Key generated by the DCA for the purposes of complying with its obligations under the Code.

DCA Personnel means those persons who are engaged by the DCC, in so far as such persons carry out, or are authorised to carry out, any function of the DCA.

DCA Private Key means a DCA Key which is a Private Key.

DCA Public Key means a DCA Key which is a Public Key.

DCA Systems means the Systems used by the DCA in relation to the SMKI Services.

DCA Certificate means either a Root DCA Certificate or an Issuing DCA Certificate.

Device Certificate means a certificate in the form set out in the Device Certificate Profile in accordance with Annex B, and Issued by the Issuing DCA in accordance with this Policy.

Device Certification Authority (or **DCA**) means the DCC, acting in the capacity and exercising the functions of one or more of:

(a) the Root DCA;

(b) the Issuing DCA; and

(c) the Registration Authority.

Eligible Subscriber means:

(a) in relation to a Device Certificate, an Authorised Subscriber which is identified as an Eligible Subscriber in accordance with Section L3.16 of the Code (Device Certificates); and

(b) in relation to a DCA Certificate, an Authorised Subscriber which is identified as an Eligible Subscriber in accordance with Section L3.17 of the Code (DCA Certificates).

Issue means the act of the DCA, in its capacity as the Root DCA or Issuing DCA, and acting in accordance with this Policy, of creating and signing a Certificate which is bound to both a Subject and a Subscriber (and "**Issued**" and "**Issuing**" shall be interpreted accordingly).

Issuing Device Certification Authority (or **Issuing DCA**) means the DCC exercising the function of Issuing Device Certificates to Eligible Subscribers and of storing and managing the Private Keys associated with that function.

Issuing DCA Certificate means a certificate in the form set out in the Issuing DCA Certificate Profile in accordance with Annex B, and Issued by the Root DCA to the Issuing DCA in accordance with this Policy.

Issuing DCA Private Key means a Private Key which is stored and managed by the DCA acting in its capacity as the Issuing DCA.

Issuing DCA Public Key means the Public Key which is part of a Key Pair with an Issuing DCA Private Key.

Key Escrow means the storage of a Private Key by a person other than the Subscriber or Subject of the Certificate which contains the related Public Key.

Object Identifier (or **OID**) means an Object Identifier assigned by the Internet Address Naming Authority.

OCA has the meaning given to that expression in Appendix B of the Code (Organisation Certificate Policy).

OCA Systems has the meaning given to that expression in Appendix B of the Code (Organisation Certificate Policy).

Policy means this Device Certificate Policy.

Private Key Material in relation to a Private Key, means that Private Key and the input parameters necessary to establish, use and maintain it.

Registration Authority means the DCC exercising the function of receiving and processing Certificate Signing Requests made in accordance with the SMKI RAPP.

Root Device Certification Authority (or **Root DCA**) means the DCC exercising the function of Issuing DCA Certificates to the Issuing DCA and storing and managing Private Keys associated with that function.

Root DCA Certificate means a certificate in the form set out in the Root DCA Certificate Profile in accordance with Annex B and self-signed by the Root DCA in accordance with this Policy.

Root DCA Private Key means a Private Key which is stored and managed by the DCA acting in its capacity as the Root DCA.

Security Related Functionality means the functionality of the DCA Systems which is designed to detect, prevent or mitigate the adverse effect of any Compromise of that System.

SMKI Registration Authority Manager has the meaning given to that expression in the SMKI RAPP.

SMKI Registration Authority Personnel has the meaning given to that expression in the SMKI RAPP.

Subject means:

(a) in relation to a Device Certificate, the Device identified by the Device ID in the `hwSerialNum` field of the Device Certificate Profile in Annex B; and

(b) in relation to a DCA Certificate, the Root DCA or Issuing DCA as identified by the `subject` field of the relevant Certificate Profile in Annex B.

Subscriber means, in relation to any Certificate, a Party or RDP which has been Issued with and accepted that Certificate, acting in its capacity as the holder of the Certificate.

Time-Stamping means the act that takes place when a Time-Stamping Authority, in relation to a Certificate, stamps a particular datum with an accurate indicator of the time (in hours, minutes and seconds) at which the activity of stamping takes place.

Time-Stamping Authority means that part of the DCA that:

(a) where required, provides an appropriately precise time-stamp in the format required by this Policy; and

(b) relies on a time source that is:

(i) accurate;

(ii) determined in a manner that is independent of any other part of the DCA Systems; and

(iii) such that the time of any time-stamp can be verified to be that of the Independent Time Source at the time at which the time-stamp was applied.

Validity Period means, in respect of a Certificate, the period of time for which that Certificate is intended to be valid.

Annex B: DCA Certificate and Device Certificate Profiles

End Entity Certificate Structure and Contents

This Annex lays out requirements as to structure and content with which DCA Certificates and Device Certificates shall comply. All terms in this Annex shall, where not defined in the Code, this Policy, or the GB Companion Specification, have the meanings in IETF RFC 5759 or IETF RFC 5280.

Common requirements applicable to DCA Certificates and Device Certificates

All DCA Certificates and Device Certificates that are validly authorised within the SMKI for use within the scope of the GB Companion Specification:

- shall be compliant with IETF RFC 5759 and so with IETF RFC 5280.
- for clarity and in adherence with the requirements of IETF RFC 5759, all DCA Certificates and Device Certificates shall:
    - contain the `authorityKeyIdentifier` extension, except where the Certificate is the Root DCA Certificate;
    - contain the `keyUsage` extension which shall be marked as critical;
- be X.509 v3 certificates as defined in IETF RFC 5280, encoded using the ASN.1 Distinguished Encoding Rules;
- only contain Public Keys of types that are explicitly allowed by the GBCS. This means all Public Keys shall be elliptic curve Public Keys on the NIST P-256 curve;
- only contain Public Keys in uncompressed form i.e. contain an elliptic curve point in uncompressed form as detailed in Section 2.2 of IETF RFC 5480;
- only provide for signature methods that are explicitly allowed within the GBCS. This means using P-256 Private Keys with SHA 256 and ECDSA;
- contain a `certificatePolicies` extension containing at least one `CertPolicyID` which shall be marked as critical. For clarity and in adherence with IETF RFC 5280, Certification Path Validation undertaken by Devices shall interpret this extension;
- contain a `serialNumber` of no more than 16 octets in length;

- contain a subjectKeyIdentifier which shall be marked as non-critical;
- contain an authorityKeyIdentifier in the form [0] KeyIdentifier which shall be marked as non-critical, except where the Certificate is the Root DCA Certificate;
- only contain KeyIdentifiers generated as per method (2) of Section 4.2.1.2 of IETF RFC 5280 and so which shall always be 8 octets in length;
- contain an issuer field whose contents MUST be identical to the contents of the signer's subject field in the signer's Certificate;
- have a valid notBefore field consisting of the time of issue encoded and a valid notAfter field for a not well-defined expiraton date as per IETF RFC 5280 Section 4.1.2.5.

Requirements applicable to Device Certificates only

All Device Certificates that are issued by the DCA shall:

- not have a well-defined expiration date and so the notAfter shall be assigned the GeneralizedTime value of 99991231235959Z;
- have an empty subject field;
- contain subjectAltName extension which contains a single GeneralName of type otherName that is further sub-typed as a hardwareModuleName (id-on-hardwareModuleName) as defined in RFC 4108 section 5. The hwSerialNum field shall be set to the Device's Entity Identifier. In adherence to IETF RFC 5280, the subjectAltName shall be marked as critical;
- contain a single Public Key;
- contain a keyUsage extension marked as critical, with a value of only one of:
    - digitalSignature; or
    - keyAgreement.
- contain a single CertPolicyID in the certificatePolicies extension that refers to the OID applicable to the version of this Device Certificate Policy applicable at the time that the Device Certificate was issued.

Requirements applicable to the Root DCA and Issuing DCA

All DCA Certificates issued by the DCA shall:

- not have a well-defined expiration date and so the notAfter shall be assigned the GeneralizedTime value of 99991231235959Z;
- must have a Valid notBefore field consisting of the time of issue encoded as per RFC 5280;
- Per RFC 5280, the IssuerName of any certificates MUST be identical to the signer's subject;
- have a globally unique subject;
- contain a single Public Key;
- contain a keyUsage extension marked as critical and defined as keyCertSign;
- For Issuing DCA Certificates contain at least one CertPolicyID in the certificatePolicies extension that refers to the OID of the version of this Device Certificate Policy prevailing at the time.
- For the Root DCA Certificate contain a single CertPolicyID in the certificatePolicies extension that refers to the OID for anyPolicy.
- For Issuing DCA Certificates, contain the basicConstraints extension, with values cA=True, and pathLen=0. This extension shall be marked as critical.
- For the Root DCA Certificate, contain the basicConstraints extension, with the value cA=True and pathLen absent (unlimited). This extension shall be marked as critical.

Device Certificate Profile

Field Name	RFC 5759/5280 Type	Value	Reference
version	INTEGER	v3	

serialNumber	INTEGER	Positive Integer of up to 16 Octets	
signature	AlgorithmIdentifier	SHA256 with ECDSA	
The value field of the AttributeTypeAndValue structure within the subject field whose type is id-at-commonName (the "Issuer X520 Common Name")	UTF8String	Globally unique common name of Issuing DCA of up to 4 Octets (as defined in the Issuing DCA Certificate Profile)	
keyIdentifier in Authoritykeyidentifier (the "Authority Key Identifier")	keyIdentifier	A unique value that matches the subjectKeyIdentifier value of the issuer's credential	
keyIdentifier in SubjectKeyIdentifier (the "Subject Key Identifier")	keyIdentifier	Provides a means for identifying certificates containing the particular Public Key used in an application	
notBefore	Time	Creation time of the Device Certificate	
notAfter	Time	shall be assigned the GeneralizedTime value of 99991231235959Z	

The value field of the AttributeTypeAndValue structure within the subject field whose type is id-at-commonName (the "Subject X520 Common Name")	UTF8String	EMPTY	
subjectAltName	OtherName	contains a single GeneralName of type OtherName that is further sub-typed as a HardwareModuleName (id-on-hardwareModuleName) as defined in RFC 4108 section 5. The hwSerialNum field shall be set to the Device's Entity Identifier	
subjectPublicKeyInfo	SubjectPublicKeyInfo	The Subject's Public Key	
extensions	Extensions	Critical and non-critical extensions	
signatureAlgorithm	AlgorithmIdentifier	SHA256 with ECDSA	
signatureValue	BIT STRING	Subject Device Certificate signature	

Interpretation

`version`

The version of the X.509 Device Certificate. Valid Device Certificates shall identify themselves as version 3.

`serialNumber`

Device Certificate serial number, a positive integer of up to 16 octets. The `serialNumber` identifies the Device Certificate, and shall be created by the Issuing DCA that signs the Device Certificate. The `serialNumber` shall be unique in the scope of Device Certificate signed by the Issuing DCA.

`signature`

The identity of the signature algorithm used to sign the Device Certificate. The field is identical to the value of the Device Certificate `signatureAlgorithm` field explained further under the next **`signatureAlgorithm`** heading below.

Issuer X520 Common Name

The name of the signer of the Device Certificate. This will be the gloablly unique name of the Issuing DCA of up to 4 Octets (as defined in the Issuing DCA Certificate Profile).

Authority Key Identifier

To optimize building the correct credential chain, the non-critical Authority Key Identifier extension shall be populated with a unique value as recommended by RFC 5280 and shall be included in all Device Certificates.

Subject Key Identifier

The Subject Key Identifier extension should be included and marked as non-critical in the Device Certificate.

`validity`

The time period over which the Issuing DCA expects the Device Certificate to be valid. The `validity` period is the period of time from `notBefore` through `notAfter`, inclusive.

Device Certificate are expected to operate indefinitely into the future and should use the value 99991231235959Z. Solutions verifying a Device Certificate are expected to accept this value indefinitely.

All times shall be stated in the Universal Coordinated Time (UTC) time zone. Times up to and including 23:59:59 December 31, 2049 UTC shall be encoded as `UTCTime` as YYMMDDHHmmssZ.

Times later than 23:59:59 December 31, 2049 UTC shall be encoded as `GeneralizedTime` as YYYYMMDDHHmmssZ.

`notBefore`

The earliest time a Device Certificate may be used. This shall be the time the Device Certificate is created.

`notAfter`

The latest time a Device Certificate is expected to be used. Device Certificate are expected to operate indefinitely into the future and should use the value 99991231235959Z. Solutions verifying a Device Certificate are expected to accept this value indefinitely.

Subject X520 Common Name

This field must be EMPTY.

`subjectAltName`

The non-critical `subjectAltName` extension shall contain a single `GeneralName` of type `OtherName` that is further sub-typed as a `HardwareModuleName` (`id-on-hardwareModuleName`) as defined in RFC 4108 section 5. The `hwSerialNum` field shall be set to the Device ID.

subjectPublicKeyInfo

The Device Certificate `subjectPublicKeyInfo` field shall indicate the Public Key algorithm identifier and the Public Key in the specified algorithm format as specified in RFC 3279 and RFC 5480.

The algorithm field in the `subjectPublicKeyInfo` structure shall contain the following identifier:

```
id-ecPublicKey OBJECT IDENTIFIER ::= {iso(1) member-body(2)
us(840) ansi-X9-62(10045) keyType(2) 1 }
```

id-ecPublicKey indicates that the algorithms that can be used with the subject Public Key are unrestricted. The key is only restricted by the values indicated in the `KeyUsage` Device Certificate extension (explained further under the next **`extensions`** heading below).

The parameter for `id-ecPublicKey` is as follows and shall always be present:

```
ECParameters ::= CHOICE {

    namedCurve          OBJECT IDENTIFIER

    -- implicitCurve   NULL

    -- specifiedCurve  SpecifiedECDomain

  }
```

Only the following field in ECParameters shall be used:

- o `namedCurve` - identifies all the required values for a particular set of elliptic curve domain parameters to be represented by an object identifier.

The `OBJECT IDENTIFIER` for the curve choice to be used in Device Certificate is:

```
secp256r1  OBJECT  IDENTIFIER  ::=  {  iso(1)  member-body(2)
us(840) ansi-X9-62(10045) curves(3) prime(1) 7 }
```

The `subjectPublicKey` from `SubjectPublicKeyInfo` is the ECC Public Key.

Implementations of Elliptic Curve Cryptography according to this document shall only support the uncompressed form.

The first octet of the `subjectPublicKey` indicates whether the key is compressed or uncompressed. The uncompressed form is indicated by 0x04 (the compressed form is indicated by either 0x02 or 0x03). The Public Key shall be rejected if any value other than 0x04 is in the first octet.

signatureAlgorithm

The `signatureAlgorithm` field shall indicate the Issuing DCA signature algorithm used to sign this Device Certificate is as defined under the next **Signature Method (ECDSA)** heading.

signatureValue

The Issuing DCA's signature of the Device Certificate shall be computed using the Issuing DCA's private signing key using the algorithm identified under the next **Signature Method (ECDSA)** heading.

The structure for ECDSA signatures shall be as per RFC 5480.

extensions

Device Certificates shall contain the extensions described below. They SHOULD NOT contain any additional `extensions`:

- `certificatePolicy`
- `subjectAltName`
- `keyUsage`
- `authorityKeyIdentifier`
- `subjectKeyIdentifier`

Cryptographic Primitives for Signature Method

Signature Method (ECDSA)

The ECDSA signature method is defined in NIST FIPS 186-4. When implementing ECDSA, the SHA-256 message digest algorithm and the P-256 elliptic curve as defined in FIPS 186-4 Annex D, D.1.2.3, shall be used.

The signature algorithm shall be `ecdsa-with-SHA256` as specified in RFC 5759. The algorithm identifier is:

```
ecdsa-with-SHA256 OBJECT IDENTIFIER ::= { iso(1) member-body(2) us(840) ansi-X9-62(10045) signatures(4) ecdsa-with-sha2(3) 2 }
```

SHA-256 hash algorithm

The hash algorithm used shall be the SHA-256 secure hash algorithm as defined in NIST FIPS 180-4.

Root DCA Certificate Profile

Field Name	RFC 5759/5280 Type	Value	Reference
`version`	`INTEGER`	v3	
`serialNumber`	`INTEGER`	Positive Integer of up to 16 Octets	
`signature`	`AlgorithmIdentifier`	SHA256 with ECDSA	
The `value` field of the `AttributeTypeAndValue` structure within the `subject` field whose `type` is `id-at-`	`UTF8String`	Globally unique common name of Root DCA of up to 4 Octets	

commonName (the “Issuer X520 Common Name”)			
keyIdentifier in subjectKeyIdentifier (the "Subject Key Identifider")	keyIdentifier	A unique value that matches the subjectKeyIdentifier of the issuer’s credential	
notBefore	Time	Creation time of the Certificate	
notAfter	Time	shall be assigned the GeneralizedTime value of 99991231235959Z	
The value field of the AttributeTypeAndValue structure within the subject field whose type is id-at-commonName (the “Subject X520 Common Name”)	UTF8String	Globally unique name of Root DCA of up to 4 Octets (same as Issuer name)	
subjectPublicKeyInfo	SubjectPublicKeyInfo	The Subject’s Public Key	
extensions	Extensions	Critical and non-critical extensions	

`signatureAlgorithm`	`AlgorithmIdentifier`	SHA256 with ECDSA	
`signatureValue`	`BIT STRING`	Subject Certificate signature	

These certificates are the root of trust for the Devices SMKI.

`version`

The version of the X.509 Certificate. Valid Certificates shall identify themselves as version 3.

`serialNumber`

Certificate serial number, a positive integer of up to 16 octets. The `serialNumber` identifies the Certificate, and shall be created by the DCA that signs the Certificate (self-signed by Root DCA). The `serialNumber` shall be unique in the scope of Certificates signed by the DCA.

`signature`

The identity of the signature algorithm used to sign the Certificate. The field is identical to the value of the Root DCA Certificate's `signatureAlgorithm` field explained further under the next signatureAlgorithm heading.

Issuer X520 Common Name

The name of the signer of the Certificate. This will be the gloablly unique name of the Root DCA of up to 4 Octets. This will be the same as the `subject` as it is self-signed by the Root DCA.

Subject Key Identifier

The `subjectKeyIdentifier` extension should be included and marked as non-critical in the Certificate.

`validity`

The time period over which the issuer expects the Certificate to be valid. The validity period is the period of time from `notBefore` through `notAfter`, inclusive.

Root DCA certificates are expected to operate indefinitely into the future and should use the value 99991231235959Z. Solutions verifying a Root DCA certificate are expected to accept this value indefinitely.

All times shall be stated in the Universal Coordinated Time (UTC) time zone. Times up to and including 23:59:59 December 31, 2049 UTC shall be encoded as `UTCTime` as YYMMDDHHmmssZ.

Times later than 23:59:59 December 31, 2049 UTC shall be encoded as `GeneralizedTime` as YYYYMMDDHHmmssZ.

`notBefore`

The earliest time a Certificate may be used. This shall be the time the Certificate is created.

`notAfter`

The latest time a Certificate is expected to be used. Certificates are expected to operate indefinitely into the future and should use the value 99991231235959Z. Solutions verifying a Certificate are expected to accept this value indefinitely.

Subject X520 Common Name

This field must be populated with the globally unique name of the Root DCA of up to 4 Octets.

`subjectPublicKeyInfo`

The Certificate's `subjectPublicKeyInfo` field shall indicate the Public Key algorithm identifier and the Public Key in the specified algorithm format as specified in RFC 3279 and RFC 5480.

The algorithm field in the `subjectPublicKeyInfo` structure shall be use the following identifier:

```
id-ecPublicKey OBJECT IDENTIFIER ::= {iso(1) member-
body(2) us(840) ansi-X9-62(10045) keyType(2) 1 }
```

`id-ecPublicKey` indicates that the algorithms that can be used with the subject Public Key are unrestricted. The key is only restricted by the values indicated in the Key Usage Certificate extension (explained further under the next **extensions** heading).

The parameter for `id-ecPublicKey` is as follows and shall always be present:

```
ECParameters ::= CHOICE {

    namedCurve         OBJECT IDENTIFIER

    -- implicitCurve   NULL

    -- specifiedCurve  SpecifiedECDomain

  }
```

Only the following field in ECParameters shall be used:

o `namedCurve` - identifies all the required values for a particular set of elliptic curve domain parameters to be represented by an `OBJECT IDENTIFIER`.

The object identifier for the curve choice to be used in DCA Certificates is:

```
secp256r1 OBJECT IDENTIFIER ::= { iso(1) member-body(2)
us(840) ansi-X9-62(10045) curves(3) prime(1) 7 }
```

The `subjectPublicKey` from `SubjectPublicKeyInfo` is the ECC Public Key.

Implementations of Elliptic Curve Cryptography according to this document shall only support the uncompressed form.

The first octet of the `subjectPublicKey` indicates whether the key is compressed or uncompressed. The uncompressed form is indicated by 0x04 (the compressed form is indicated by either 0x02 or 0x03). The Public Key shall be rejected if any value other than 0x04 is in the first octet.

`signatureAlgorithm`

The `signatureAlgorithm` field shall indicate the Root DCA signature algorithm used to sign this Certificate as defined under the next **Signature Method (ECDSA)** heading.

`signatureValue`

The Root DCA's signature of the Certificate shall be computed using the Root DCA's private signing key using the algorithm identified under the next **Signature Method (ECDSA)** heading .

The structure for ECDSA signatures shall be as per RFC 5480.

`extensions`

Certificates MUST contain the extensions described below and MUST have the name form as described. They SHOULD NOT contain any additional extensions:

Extensions:

- `certificatePolicy`
- `keyUsage`
- `basicConstraints`
- `subjectKeyIdentifer`

Cryptographic Primitives for Signature Method

Signature Method (ECDSA)

The ECDSA signature method is defined in NIST FIPS 186-4. When implementing ECDSA, the SHA-256 message digest algorithm and the P-256 elliptic curve as defined in FIPS 186-4 Annex D, D.1.2.3, shall be used.

The signature algorithm shall be `ecdsa-with-SHA256` as specified in RFC 5759. The algorithm identifier is:

```
ecdsa-with-SHA256 OBJECT IDENTIFIER ::= { iso(1) member-body(2) us(840) ansi-X9-62(10045) signatures(4) ecdsa-with-sha2(3) 2 }
```

SHA-256 hash algorithm

The hash algorithm shall be the SHA-256 secure hash algorithm as defined in NIST FIPS 180-4.

Issuing DCA Certificate Profile

Field Name	RFC 5759/5280 Type	Value	Reference
version	INTEGER	v3	
serialNumber	INTEGER	Positive Integer of up to 16 Octets	
signature	AlgorithmIdentifier	SHA256 with ECDSA	
The value field of the AttributeTypeAndValue structure within the subject field whose type is id-at-commonName (the "Issuer X520 Common Name")	UTF8String	Globally unique name of Root DCA of up to 4 Octets (as defined in the Root DCA Certificate Profile)	
keyIdentifier in subjectKeyIdentifier (the "Subject Key Identifier")	keyIdentifier	Provides a means for identifying certificates containing the particular Public Key used in an application	

keyIdentifier in authorityKeyIdentifier (the "Authority Key Identifier")	keyIdentifier	A unique value that matches the subjectKeyIdentifier value of the issuer's credential	
notBefore	Time	Creation time of the certificate	
notAfter	Time	shall be assigned the GeneralizedTime value of 99991231235959Z	
The value field of the AttributeTypeAndValue structure within the subject field whose type is id-at-commonName (the "Subject X520 Common Name")	UTF8String	Globally unique name of Issuing DCA of up to 4 Octets	
subjectPublicKeyInfo	SubjectPublicKeyInfo	The Subject's Public Key	
extensions	Extensions	Critical and non-critical extensions	
signatureAlgorithm	AlgorithmIdentifier	SHA256 with ECDSA	
signatureValue	BIT STRING	Subject certificate signature	

`version`

The version of the X.509 Certificate. Valid Certificates shall identify themselves as version 3.

`serialNumber`

Certificate serial number, a positive integer of up to 16 octets. The `serialNumber` identifies the Certificate, and shall be created by the Issuing DCA that signs the Certificate. The `serialNumber` shall be unique in the scope of Certificates signed by the Root DCA.

`signature`

The identity of the signature algorithm used to sign the Certificate. The field is identical to the value of the Issuing DCA Certificate's `signatureAlgorithm` field explained further under the next **signatureAlgorithm** heading.

Issuer X520 Common Name

The name of the signer of the Certificate. This will be the gloablly unique name of the Root DCA of up to 4 Octets (as defined in the Root DCA Certificate Profile).

Subject Key Identifier

The `subjectKeyIdentifier` extension should be included and marked as non-critical in the Certificate.

Authority Key Identifier

To optimize building the correct credential chain, the non-critical `authorityKeyIdentifier` extension shall be populated with a unique value as recommended by RFC 5280 and shall be included in all device Certificates.

`validity`

The time period over which the issuer expects the Certificate to be valid. The `validity` period is the period of time from `notBefore` through `notAfter`, inclusive.

Issuing DCA certificates are expected to operate indefinitely into the future and should use the value 99991231235959Z. Solutions verifying a Issuing DCA certificate are expected to accept this value indefinitely.

All times shall be stated in the Universal Coordinated Time (UTC) time zone. Times up to and including 23:59:59 December 31, 2049 UTC shall be encoded as `UTCTime` as YYMMDDHHmmssZ.

Times later than 23:59:59 December 31, 2049 UTC shall be encoded as `GeneralizedTime` as YYYYMMDDHHmmssZ.

`notBefore`

The earliest time a Certificate may be used. This shall be the time the Certificate is created.

`notAfter`

The latest time a Certificate is expected to be used. Certificates are expected to operate indefinitely into the future and should use the value 99991231235959Z. Solutions verifying a Certificate are expected to accept this value indefinitely.

Subject X520 Common Name

This field shall be populated with the globally unique name of the Issuing DCA of up to 4 Octets.

`subjectPublicKeyInfo`

The Certificate's `subjectPublicKeyInfo` field shall indicate the Public Key algorithm identifier and the Public Key in the specified algorithm format as specified in RFC 3279 and RFC 5480.

The algorithm field in the `subjectPublicKeyInfo` structure shall contain the following identifier:

```
id-ecPublicKey OBJECT IDENTIFIER ::= {iso(1) member-body(2)
us(840) ansi-X9-62(10045) keyType(2) 1 }
```

`id-ecPublicKey` indicates that the algorithms that can be used with the subject Public Key are unrestricted. The key is only restricted by the values indicated in the key usage Certificate extension (explained further under the next **extensions** heading).

The parameter for `id-ecPublicKey` is as follows and shall always be present:

```
  ECParameters ::= CHOICE {

       namedCurve          OBJECT IDENTIFIER

       -- implicitCurve    NULL

       -- specifiedCurve   SpecifiedECDomain

     }
```

Only the following field in ECParameters shall be used:

o `namedCurve` - identifies all the required values for a particular

set of elliptic curve domain parameters to be represented by an

`OBJECT IDENTIFIER`.

The object identifier for the curve choice to be used in Certificates is:

```
secp256r1  OBJECT  IDENTIFIER  ::=  {  iso(1)  member-body(2)
us(840) ansi-X9-62(10045) curves(3) prime(1) 7 }
```

The `subjectPublicKey` from `SubjectPublicKeyInfo` is the ECC Public Key.

Implementations of Elliptic Curve Cryptography according to this document shall only support the uncompressed form.

The first octet of the `subjectPublicKey` indicates whether the key is compressed or uncompressed. The uncompressed form is indicated by 0x04 (the compressed form is indicated by either 0x02 or 0x03). The Public Key MUST be rejected if any value other than 0x04 is included in the first octet.

`signatureAlgorithm`

The `signatureAlgorithm` field shall indicate the Root DCA signature algorithm used to sign this Certificate as defined under the next **Signature Method (ECDSA)** heading.

`signatureValue`

The Root DCA's signature of the Certificate shall be computed using the Root DCA's private signing key using the algorithm identified under the next **Signature Method (ECDSA)** heading.

The structure for ECDSA signatures shall be as per RFC 5480.

`extensions`

Issuing-CA certificates shall contain the `extensions` described below. They SHOULD NOT contain any additional extensions:

- `certificatePolicy`
- `keyUsage`
- `basicConstraints`
- `subjectKeyIdentifer`
- `authorityKeyIdentifier`
- `subjectAltName`

Cryptographic Primitives for Signature Method

Signature Method (ECDSA)

The ECDSA signature method is defined in NIST FIPS 186-4. When implementing ECDSA, the SHA-256 message digest algorithm and the P-256 elliptic curve as defined in FIPS 186-4 Annex D, D.1.2.3, shall be used.

The signature algorithm shall be `ecdsa-with-SHA256` as specified in RFC 5759. The algorithm identifier is:

```
ecdsa-with-SHA256 OBJECT IDENTIFIER ::= { iso(1) member-
body(2) us(840) ansi-X9-62(10045) signatures(4) ecdsa-with-
sha2(3) 2 }
```

SHA-256 hash algorithm

The hash algorithm used shall be the SHA-256 secure hash algorithm as defined in NIST FIPS 180-4.

Version B 10.0

Appendix B

Organisation Certificate Policy

CONTENTS

Part Heading Page

1 INTRODUCTION

The document comprising this Appendix B (together with its Annexes A and B):

- shall be known as the "**Organisation Certificate Policy**" (and in this document is referred to simply as the "**Policy**"),
- is a SEC Subsidiary Document related to Section L9 of the Code (The SMKI Document Set).

1.1 OVERVIEW

(A) This Policy sets out the arrangements relating to:

(i) Organisation Certificates; and

(ii) OCA Certificates.

(B) This Policy is structured according to the guidelines provided by IETF RFC 3647, with appropriate extensions, modifications and deletions.

(C) Except where the context otherwise requires, words or expressions used in this Policy shall have the meanings ascribed to them in IETF RFC 5280 where they:

(i) appear in `Courier New` font;

(ii) are accompanied by the descriptor 'field', 'type' or 'extension'; and/or

(iii) take the form of a conjoined string of two or more words, such as '`digitalSignature`'.

1.2 DOCUMENT NAME AND IDENTIFICATION

(A) This Policy has been assigned an OID of 1.2.826.0.1. 8641679.1.2.1.1.

1.3 SMKI PARTICIPANTS

1.3.1 The Organisation Certification Authority

(A) The definition of Organisation Certification Authority is set out in Annex A.

1.3.2 Registration Authorities

(A) The definition of Registration Authority is set out in Annex A.

1.3.3 Subscribers

(A) In accordance with Section L3 of the Code (The SMKI Services), certain Parties may become Authorised Subscribers.

(B) In accordance with Section L3 of the Code (The SMKI Services), an Authorised Subscriber shall be an Eligible Subscriber in relation to certain Certificates.

(C) The SMKI RAPP sets out the procedure to be followed by an Eligible Subscriber in order to become a Subscriber for one or more Certificates.

(D) Eligible Subscribers are subject to the applicable requirements of the SMKI RAPP and Section L11 of the Code (Subscriber Obligations).

(E) Obligations on the DCC acting in the capacity of an Eligible Subscriber are set out in Section L11 of the Code (Subscriber Obligations).

(F) The definitions of the following terms are set out in Section A of the Code (Definitions and Interpretation):

(i) Authorised Subscriber;

(ii) Eligible Subscriber;

(iii) Subscriber.

1.3.4 Subjects

(A) The Subject of an Organisation Certificate must be an Organisation and be identified in the `subject` field of the Organisation Certificate Profile in accordance with Annex B.

(B) The Subject of an OCA Certificate must be the entity identified by the subject field of the Root OCA Certificate Profile or Issuing OCA Certificate Profile (as the case may be) in accordance with Annex B.

(C) The definition of Subject is set out in Annex A.

1.3.5 Relying Parties

(A) In accordance with Section L12 of the Code, certain Parties may be Relying Parties.

(B) Relying Parties are subject to the applicable requirements of Section L12 of the Code (Relying Party Obligations).

(C) Obligations on the DCC acting in the capacity of a Relying Party are set out in Section L12 of the Code (Relying Party Obligations).

(D) The definition of Relying Party is set out in Annex A.

1.3.6 SMKI Policy Management Authority

(A) Provision in relation to the SMKI PMA is made in Section L1 of the Code (SMKI Policy Management Authority).

1.3.7 SMKI Repository Provider

(A) Provision in relation to the SMKI Repository Service is made in Section L5 of the Code (The SMKI Repository Service).

1.4 USAGE OF ORGANISATION CERTIFICATES AND OCA CERTIFICATES

1.4.1 Appropriate Certificate Uses

(A) The OCA shall ensure that Organisation Certificates are Issued only:

(i) to Eligible Subscribers; and

(ii) for the purposes of the creation, sending, receipt and processing of communications to and from Organisations in accordance with or pursuant to the Code.

(B) The OCA shall ensure that OCA Certificates are Issued only to the OCA:

(i) in its capacity as, and for the purposes of exercising the functions of, the Root OCA; and

(ii) in its capacity as, and for the purposes of exercising the functions of, the Issuing OCA.

(C) Further provision in relation to the use of Certificates is made in Section L11 (Subscriber Obligations) and Section L12 (Relying Party Obligations) of the Code.

1.4.2 Prohibited Certificate Uses

(A) No Party or RDP shall use a Certificate other than for the purposes specified in Part 1.4.1 of this Policy.

1.5 POLICY ADMINISTRATION

1.5.1 Organisation Administering the Document

(A) This Policy is a SEC Subsidiary Document and is administered as such in accordance with the provisions of the Code.

1.5.2 Contact Person

(A) Questions in relation to the content of this Policy should be addressed to the OCA or the SMKI PMA.

1.5.3 Person Determining Organisation CPS Suitability for the Policy

(A) Provision is made in Section L9.14 (d) of the Code for the SMKI PMA to approve the Organisation CPS.

1.5.4 Organisation CPS Approval Procedures

(A) Provision is made in Section L9.15 of the Code for the procedure by which the SMKI PMA may approve the Organisation CPS.

1.5.5 Registration Authority Policies and Procedures

(A) The SMKI Registration Authority Policies and Procedures (the **SMKI RAPP**) are set out at Appendix D of the Code.

1.6 DEFINITIONS AND ACRONYMS

1.6.1 Definitions

(A) Definitions of the expressions used in this Policy are set out in Section A of the Code (Definitions and Interpretation) and Annex A.

1.6.2 Acronyms

(A) Any acronyms used for the purposes of this Policy are set out in Section A of the Code (Definitions and Interpretation) and Annex A.

2 PUBLICATION AND REPOSITORY RESPONSIBILITIES

2.1 REPOSITORIES

(A) Provision is made in Section L5 of the Code (The SMKI Repository Service) for the establishment, operation and maintenance of the SMKI Repository.

2.2 PUBLICATION OF CERTIFICATION INFORMATION

(A) The OCA shall lodge copies of the following in the SMKI Repository:

(i) each Organisation Certificate that has been accepted by a Subscriber;

(ii) each OCA Certificate;

(iii) each version of the SMKI RAPP;

(iv) each version of the SMKI Recovery Procedure;

(v) the latest version of the Organisation CRL;

(vi) the latest version of the Organisation ARL; and

(vii) any other document or information that may from time to time be specified, for the purposes of this provision, by the SMKI PMA.

(B) The OCA may lodge in the SMKI Repository such other documents or information as it may from time to time consider appropriate.

(C) Further provision on the lodging of documents and information in the SMKI Repository is made in Section L5 of the Code (The SMKI Repository Service).

2.3 TIME OR FREQUENCY OF PUBLICATION

(A) The OCA shall ensure that:

(i) each Organisation Certificate is lodged in the SMKI Repository promptly on its acceptance by a Subscriber;

(ii) each OCA Certificate is lodged to the SMKI Repository promptly on being Issued;

(iii) the Policy is lodged in the SMKI Repository, and a revised version of the Policy is lodged in the SMKI Repository promptly following each modification to it made in accordance with the Code;

(iv) the SMKI RAPP is lodged in the SMKI Repository, and a revised version of the SMKI RAPP is lodged in the SMKI Repository promptly following each modification to it made in accordance with the Code;

(v) the SMKI Recovery Procedure is lodged in the SMKI Repository, and a revised version of the SMKI Recovery Procedure is lodged in the SMKI Repository promptly following each modification to it made in accordance with the Code;

(vi) the Organisation CRL is lodged in the SMKI Repository, and a revised version of the Organisation CRL is lodged in the SMKI Repository within such time as is specified in Part 4.9.7 of this Policy;

(vii) the Organisation ARL is lodged in the SMKI Repository, and a revised version of the Organisation ARL is lodged in the SMKI Repository within such time as is specified in Part 4.9.7 of this Policy; and

(viii) any other document that may from time to time be specified by the SMKI PMA is lodged in the SMKI Repository within such time as may be directed by the SMKI PMA.

2.4 ACCESS CONTROLS ON REPOSITORIES

(A) Provision in relation to access controls for the SMKI Repository is made in Sections L5.5, L5.6 and L5.6A of the Code.

3 IDENTIFICATION AND AUTHENTICATION

3.1 NAMING

3.1.1 Types of Names

(A) Provision is made in the SMKI RAPP to ensure that the name of the entity that is the Subject of each Certificate is in accordance with the relevant Certificate Profile at Annex B.

3.1.2 Need for Names to be Meaningful

(A) Provision is made in the SMKI RAPP to ensure that the name of the Subject of each OCA Certificate is meaningful and consistent with the relevant Certificate Profile in Annex B.

3.1.3 Anonymity or Pseudonymity of Subscribers

(A) Provision is made in the SMKI RAPP to:

(i) prohibit Eligible Subscribers from requesting the Issue of a Certificate anonymously or by means of a pseudonym; and

(ii) permit the OCA to Authenticate each Eligible Subscriber.

3.1.4 Rules for Interpreting Various Name Forms

(A) Provision in relation to name forms is made in Annex B.

3.1.5 Uniqueness of Names

(A) Provision in relation to the uniqueness of names is made in Annex B.

3.1.6 Recognition, Authentication, and Role of Trademarks

(A) Provision in relation to the use of trademarks, trade names and other restricted information in Certificates is made in Section L11 of the Code (Subscriber Obligations).

3.2 INITIAL IDENTITY VALIDATION

3.2.1 Method to Prove Possession of Private Key

(A) Provision is made in the SMKI RAPP in relation to:

(i) the procedure to be followed by an Eligible Subscriber in order to prove its possession of the Private Key which is associated with the Public Key to be contained in any Certificate that is the subject of a Certificate Signing Request; and

(ii) the procedure established for this purpose is in accordance with the procedure in PKCS#10.

3.2.2 Authentication of Organisation Identity

(A) Provision is made in the SMKI RAPP section 5.5 in relation to the:

(i) procedure to be followed by a Party or RDP in order to become an Authorised Subscriber;

(ii) criteria in accordance with which the OCA will determine whether a Party or RDP is entitled to become an Authorised Subscriber; and

(iii) requirement that the Party or RDP shall be Authenticated by the OCA for that purpose.

(B) Provision is made in the SMKI RAPP section 5.1 to ensure that each Eligible Subscriber has one or more DCC ID, User ID or RDP ID that is EUI-64 Compliant and has been allocated to that Eligible Subscriber in accordance with Section B2 (DCC, User and RDP Identifiers).

(C) Provision is made in the SMKI RAPP section 5 for the purpose of ensuring that the criteria in accordance with which the OCA shall Authenticate a Party or RDP shall be set to the level pursuant to the SMKI PMA Guidance on “Verifying Organisation Identity” published on the Website.

3.2.3 Authentication of Individual Identity

(A) Provision is made in the SMKI RAPP sections 5.2 and 5.3 in relation to the Authentication of persons engaged by Authorised Subscribers, which provides for all such persons to have their identity and authorisation verified to the level pursuant to the SMKI PMA Guidance on “Verifying Individual Identity” published on the Website.

3.2.4 Non-verified Subscriber Information

(A) The OCA shall verify all information in relation to Certificates.

(B) Further provision on the content of OCA Certificates is made in Section L11 of the Code (Subscriber Obligations).

3.2.5 Validation of Authority

See Part 3.2.2 of this Policy.

3.2.6 Criteria for Interoperation

[*Not applicable in this Policy*]

3.3 IDENTIFICATION AND AUTHENTICATION FOR RE-KEY REQUESTS

3.3.1 Identification and Authentication for Routine Re-Key

(A) This Policy does not support Certificate Re-Key.

(B) The OCA shall not provide a Certificate Re-Key service.

3.3.2 Identification and Authentication for Re-Key after Revocation

[*Not applicable in this Policy*]

3.4 IDENTIFICATION AND AUTHENTICATION FOR REVOCATION REQUEST

3.4.1 Authentication for Certificate Revocation Requests

(A) Provision is made in the SMKI RAPP section 8.2.2 in relation to procedures designed to ensure the Authentication of persons who submit a Certificate Revocation Request and verify that they are authorised to submit that request.

4 CERTIFICATE LIFE-CYCLE OPERATIONAL REQUIREMENTS

4.1 CERTIFICATE APPLICATION

4.1.1 Submission of Certificate Applications

(A) Provision is made in the SMKI RAPP in relation to:

(i) in respect of an Organisation Certificate:

(a) the circumstances in which an Eligible Subscriber may submit a Certificate Signing Request; and

(b) the means by which it may do so, including through the use of an authorised System.

4.1.2 Enrolment Process and Responsibilities

(A) Provision is made, where applicable, in the SMKI RAPP sections 5 and 6 in relation to the:

(i) establishment of an enrolment process in respect of organisations, individuals, Systems and Devices in order to Authenticate them and verify that they are authorised to act on behalf of an Authorised Subscriber or Eligible Subscriber in its capacity as such; and

(ii) maintenance by the OCA of a list of organisations, individuals, Systems and Devices enrolled in accordance with that process.

4.1.3 Enrolment Process for the Registration Authority and its Representatives

(A) Provision is made in the SMKI RAPP section 6 in relation to the establishment of an enrolment process in respect of OCA Personnel and OCA Systems:

(i) in order to Authenticate them and verify that they are authorised to act on behalf of the OCA in its capacity as the Registration Authority; and

(ii) including in particular, for that purpose, provision:

(a) for the face-to-face or video link Authentication of all SMKI Registration Authority Personnel by a SMKI Registration Authority Manager; and

(b) for all SMKI Registration Authority Personnel to have their identify and authorisation verified to the level pursuant to the SMKI PMA Guidance on "Verifying Individual Identity" published on the Website.

4.2 CERTIFICATE APPLICATION PROCESSING

4.2.1 Performing Identification and Authentication Functions

(A) Provision is made in the SMKI RAPP section 5 in relation to the Authentication by the OCA of Eligible Subscribers which submit a Certificate Signing Request.

4.2.2 Approval or Rejection of Certificate Applications

(A) Where any Certificate Signing Request fails to satisfy the requirements set out in the SMKI RAPP, the SMKI Interface Design Specification (SMKI IDS), this Policy or any other provision of the Code, the OCA:

(i) shall reject it and refuse to Issue the Certificate which was the subject of the Certificate Signing Request; and

(ii) shall give notice to the Party or RDP which made the Certificate Signing Request of the reasons for its rejection.

(B) Where any Certificate Signing Request satisfies the requirements set out in the SMKI RAPP, the SMKI IDS, this Policy or any other provision of the Code, the OCA shall Issue the Certificate which was the subject of the Certificate Signing Request.

4.2.3 Time to Process Certificate Applications

(A) Provision in relation to the performance of the SMKI Services by the OCA is made in Section L8 of the Code (SMKI Performance Standards and

Demand Management).

4.3 CERTIFICATE ISSUANCE

4.3.1 OCA Actions during Certificate Issuance

(A) The OCA may Issue a Certificate only:

(i) in accordance with the provisions of this Policy, the SMKI RAPP and the SMKI IDS; and

(ii) in response to a Certificate Signing Request made by an Eligible Subscriber in accordance with the SMKI RAPP.

(B) The OCA shall ensure that:

(i) each OCA Certificate Issued by it contains information that it has verified to be correct and complete; and

(ii) each Organisation Certificate Issued by it contains information consistent with the information in the Certificate Signing Request.

(C) An OCA Certificate may only be:

(i) Issued by the OCA; and

(ii) for that purpose, signed using the Root OCA Private Key.

(D) An Organisation Certificate may only be:

(i) Issued by the OCA; and

(ii) for that purpose, signed using an Issuing OCA Private Key.

(E) The OCA shall not Issue:

(i) an Issuing OCA Certificate using a Root OCA Private Key after the expiry of the Validity Period of a Root OCA Certificate containing the Public Key associated with that Private Key;

(ii) an Organisation Certificate using an Issuing OCA Private Key after the expiry of the Validity Period of an Issuing OCA Certificate containing the Public Key associated with that Private Key; or

(iii) any Certificate containing a Public Key where it is aware that the Public Key is the same as the Public Key contained in any other Certificate that was previously Issued by it (except that the OCA may Issue an OCA Root Certificate containing the same Public Key in so far as it contains a different, or differently encrypted, Contingency Public Key).

4.3.2 Notification to Eligible Subscriber by the OCA of Issuance of Certificate

(A) Provision is made in the SMKI IDS sections 2.3.1.4 (c) and 2.6.1.4 (d) for the OCA to notify an Eligible Subscriber where that Eligible Subscriber is Issued with a Certificate which was the subject of a Certificate Signing Request made by it.

4.4 CERTIFICATE ACCEPTANCE

4.4.1 Conduct Constituting Certificate Acceptance

(A) Provision is made in the SMKI IDS to:

(i) Specify a means by which an Eligible Subscriber may clearly indicate to the OCA its rejection of a Certificate which has been Issued to it (SMKI IDS sections 2.3.1.5 and 2.6.1.5); and

(ii) ensure that each Eligible Subscriber to which a Certificate has been Issued, and which has not rejected it, is treated as having accepted that Certificate (SMKI IDS section 2.2).

(B) A Certificate which has been Issued by the OCA shall not be treated as valid for any purposes of this Policy or the Code until it is treated as having been accepted by the Eligible Subscriber to which it was Issued.

(C) The OCA shall maintain a record of all Certificates which have been Issued by it and are treated as accepted by a Subscriber.

(D) Further provision in relation to the rejection and acceptance of Certificates is made in Section L11.5 of the Code.

4.4.2 Publication of Certificates by the OCA

(A) Provision in relation to the publication of Certificates is made in Part 2 of this Policy (Publication and Repository Responsibilities) and Section L5 of the Code (The SMKI Repository Service).

4.4.3 Notification of Certificate Issuance by the OCA to Other Entities

(A) The OCA shall give notice of the Issue of a Certificate only to the Eligible Subscriber which submitted a Certificate Signing Request in respect of that Certificate (SMKI IDS sections 2.3.1.4 and 2.6.1.4).

4.5 KEY PAIR AND CERTIFICATE USAGE

4.5.1 Subscriber Private Key and Certificate Usage

(A) Provision for restrictions on the use by Subscribers of Private Keys in respect of Certificates is made in:

(i) Section L11.8 of the Code; and

(ii) this Policy.

4.5.2 Relying Party Public Key and Certificate Usage

(A) Provision in relation to reliance that may be placed on a Certificate is made in Section L12 of the Code (Relying Party Obligations).

4.6 CERTIFICATE RENEWAL

4.6.1 Circumstances of Certificate Renewal

(A) This Policy does not support the renewal of Certificates.

(B) The OCA may only replace, and shall not renew, any Certificate.

4.6.2 Circumstances of Certificate Replacement

(A) Where the OCA Systems or any OCA Private Key is (or is suspected by the

OCA of being) Compromised, the OCA shall:

(i) immediately notify the SMKI PMA;

(ii) provide the SMKI PMA with all the information known to it in relation to the nature and circumstances of the event of Compromise or suspected Compromise; and

(iii) where the Compromise or suspected Compromise relates to an OCA Private Key (but subject to the provisions of the SMKI Recovery Procedure):

(a) ensure that the Private Key is no longer used;

(b) promptly notify each of the Subscribers for any Organisation Certificates Issued using that Private Key; and

(c) promptly both notify the SMKI PMA and, subject to the provisions of the SMKI Recovery Procedure, verifiably destroy the OCA Private Key Material.

(B) Where the OCA Root Private Key is Compromised (or is suspected by the OCA of being Compromised), the OCA:

(i) may issue a replacement for any OCA Certificate that has been Issued using that Private Key; and

(ii) shall ensure that the Subscriber for that OCA Certificate applies for the Issue of a new Certificate in accordance with this Policy.

(C) A Subscriber for an Organisation Certificate may request a replacement for that Certificate at any time by applying for the Issue of a new Organisation Certificate in accordance with this Policy.

4.6.3 Who May Request a Replacement Certificate

See Part 4.1 of this Policy.

4.6.4 Processing Replacement Certificate Requests

See Part 4.2 of this Policy

4.6.5 Notification of Replacement Certificate Issuance to a Subscriber

See Part 4.3.2 of this Policy.

4.6.6 Conduct Constituting Acceptance of a Replacement Certificate

See Part 4.4.1 of this Policy.

4.6.7 Publication of a Replacement Certificate by the OCA

See Part 4.4.2 of this Policy.

4.6.8 Notification of Certificate Issuance by the OCA to Other Entities

See Part 4.4.3 of this Policy

4.7 CERTIFICATE RE-KEY

4.7.1 Circumstances for Certificate Re-Key

(A) This Policy does not support Certificate Re-Key.

(B) The OCA shall not provide a Certificate Re-Key service.

(C) Where a new Key Pair has been generated for use by the Subject of an Organisation Certificate, the Subscriber for a Certificate which is associated with the previous Key Pair shall apply for the Issue of a new Certificate in accordance with this Policy.

4.7.2 Who may Request Certification of a New Public Key

[*Not applicable in this Policy*]

4.7.3 Processing Certificate Re-Keying Requests

[*Not applicable in this Policy*]

4.7.4 Notification of New Certificate Issuance to Subscriber

[*Not applicable in this Policy*]

4.7.5 Conduct Constituting Acceptance of a Re-Keyed Certificate

[*Not applicable in this Policy*]

4.7.6 Publication of the Re-Keyed Certificate by the OCA

[*Not applicable in this Policy*]

4.7.7 Notification of Certificate Issuance by the OCA to Other Entities

[*Not applicable in this Policy*]

4.8 CERTIFICATE MODIFICATION

4.8.1 Circumstances for Certificate Modification

(A) This Policy does not support Certificate modification (except to the extent to which it permits the OCA to Issue an OCA Root Certificate containing the same Public Key as a Certificate previously Issued by it, where the Certificates contain different, or differently encrypted, Contingency Public Keys).

(B) Subject to paragraph (A), neither the OCA nor any Subscriber may modify a Certificate.

4.8.2 Who may request Certificate Modification

[*Not applicable in this Policy*]

4.8.3 Processing Certificate Modification Requests

[*Not applicable in this Policy*]

4.8.4 Notification of New Certificate Issuance to Subscriber

[*Not applicable in this Policy*]

4.8.5 Conduct Constituting Acceptance of Modified Certificate

[*Not applicable in this Policy*]

4.8.6 Publication of the Modified Certificate by the OCA

[*Not applicable in this Policy*]

4.8.7 Notification of Certificate Issuance by the OCA to Other Entities

[*Not applicable in this Policy*]

4.9 CERTIFICATE REVOCATION AND SUSPENSION

4.9.1 Circumstances for Revocation

(A) A Subscriber shall ensure that it submits a Certificate Revocation Request in relation to a Certificate:

(i) (subject to the provisions of the SMKI Recovery Procedure) immediately upon becoming aware that the Certificate has been Compromised, or is suspected of having been Compromised, due to the Compromise of the Private Key associated with the Public Key contained within that Certificate;

(ii) immediately upon ceasing to be an Eligible Subscriber in respect of that Certificate; provided that, where a Supplier of Last Resort has been appointed in relation to premises supplied by the Subscriber, the Subscriber shall not submit a Certificate Revocation Request; or

(iii) (where the Subscriber is a Gas Network Party) immediately upon intending to cease to be a DCC User.

(B) The OCA must revoke a Certificate upon:

(i) (subject to the provisions of the SMKI Recovery Procedure) receiving a Certificate Revocation Request if the Certificate to which that request relates has been Authenticated in accordance with Part 3.4.1 of this Policy; or

(ii) being directed to do so by the SMKI PMA.

(C) The OCA must revoke a Certificate in relation to which it has not received a

Certificate Revocation Request:

(i) (subject to the provisions of the SMKI Recovery Procedure) where it becomes aware that the Certificate has been Compromised, or is suspected of having been Compromised, due to the Compromise of the Private Key associated with the Public Key contained within that Certificate;

(ii) (subject to the Section L16.11 (Supplier of Last Resort) of the Code) where it has determined that the Subscriber for that Certificate does not continue to satisfy the criteria set out in this Policy and the SMKI RAPP for being an Authorised Subscriber;

(iii) (subject to the Section L16.1 (Supplier of Last Resort) of the Code) where it becomes aware that the Subscriber for that Certificate has ceased to be an Eligible Subscriber in respect of the Certificate.

(D) In an extreme case, where it considers it necessary to do so for the purpose of preserving the integrity of the SMKI Services, the OCA may, on the receipt of a Certificate Revocation Request in relation to a Certificate which has not been Authenticated in accordance with Part 3.4.1 of this Policy, revoke that Certificate.

(E) Where the OCA revokes a Certificate in accordance with paragraph (D) it shall notify the SMKI PMA and provide a statement of its reasons for the revocation.

4.9.2 Who can Request Revocation

(A) Any Subscriber may submit a Certificate Revocation Request in relation to a Certificate for which it is the Subscriber, and shall on doing so:

(i) provide all the information specified in the SMKI RAPP section 8.2.2 (including all the information necessary for the Authentication of the Certificate); and

(ii) specify its reason for submitting the Certificate Revocation Request (which shall be a reason consistent with Part 4.9.1(A) of this Policy).

(B) The SMKI PMA may direct the OCA to revoke a Certificate.

(C) The OCA may elect to revoke a Certificate in accordance with Part 4.9.1(D) of this Policy.

4.9.3 Procedure for Revocation Request

(A) Provision is made in the SMKI RAPP section 8.2.2 in relation to the procedure for submitting and processing a Certificate Revocation Request.

(B) On receiving a Certificate Revocation Request, the OCA shall take reasonable steps to:

(i) Authenticate the Subscriber making that request;

(ii) Authenticate the Certificate to which the request relates; and

(iii) confirm that a reason for the request has been specified in accordance with Part 4.9.2 of this Policy.

(C) Where the OCA, in accordance with Part 4.9.1(C) of this Policy, intends to revoke a Certificate in relation to which it has not received a Certificate Revocation Request, it shall use its best endeavours prior to revocation to confirm with the Subscriber for that Certificate the circumstances giving rise to the revocation.

(D) The OCA shall inform the Subscriber for a Certificate where that Certificate has been revoked.

4.9.4 Revocation Request Grace Period

[*Not applicable in this Policy*]

4.9.5 Time within which OCA must process the Revocation Request

(A) The OCA shall ensure that it processes all Certificate Revocation Requests as soon as practicable, and in any event in accordance with such time as is specified in the SMKI RAPP section 8.2.2.

4.9.6 Revocation Checking Requirements for Relying Parties

(A) Provision in relation to the revocation checking requirements for Relying Parties is made in Section L12.3 of the Code.

4.9.7 CRL Issuance Frequency (if applicable)

(A) The OCA shall ensure that an up to date version of the Organisation ARL is lodged in the SMKI Repository:

(i) at least once in every period of twelve months; and

(ii) promptly on the revocation of an OCA Certificate.

(B) Each version of the Organisation ARL shall be valid until the date which is up to 13 months after the date on which that version of the Organisation ARL is lodged in the SMKI Repository.

(C) Further provision in relation to the reliance that may be placed on the Organisation ARL (and on versions of it) is set out in Section L12 of the Code (Relying Party Obligations).

(D) The OCA shall ensure that an up to date version of the Organisation CRL is lodged in the SMKI Repository:

(i) at least once in every period of twelve hours; and

(ii) within one hour on the revocation of an Organisation Certificate.

(E) Each version of the Organisation CRL shall be valid until 48 hours from the time at which it is lodged in the SMKI Repository.

(F) Further provision in relation to the reliance that may be placed on the Organisation CRL (and on versions of it) is set out in Section L12 of the Code (Relying Party Obligations).

(G) The OCA shall ensure that each up to date version of the Organisation ARL and Organisation CRL:

(i) continues to include each relevant revoked Certificate until such time as the Validity Period of that Certificate has expired; and

(ii) does not include any revoked Certificate after the Validity Period of that Certificate has expired.

(H) The OCA shall ensure that the Organisation CRL contains a non-critical entry extension which identifies the reason for the revocation of each Certificate listed on it in accordance with RFC 5280 (section 5.3.1).

(I) The OCA shall retain a copy of the information contained in all versions of the Organisation CRL and Organisation ARL, together with the dates and times between which each such version was valid. This information shall be made available as soon as is reasonably practicable, on receipt of a request, to the Panel, the SMKI PMA, any Subscriber or any Relying Party.

4.9.8 Maximum Latency for CRLs (if applicable)

See Part 4.9.7 of this Policy.

4.9.9 On-line Revocation/Status Checking Availability

(A) This Policy does not support on-line revocation status checking.

(B) The OCA shall not provide any on-line revocation status checking service.

4.9.10 On-line Revocation Checking Requirements

[*Not applicable in this Policy*]

4.9.11 Other Forms of Revocation Advertisements Available

[*Not applicable in this Policy*]

4.9.12 Special Requirements in the Event of Key Compromise

See Part 4.6.2 of this Policy.

4.9.13 Circumstances for Suspension

[*Not applicable in this Policy*]

4.9.14 Who can Request Suspension

[*Not applicable in this Policy*]

4.9.15 Procedure for Suspension Request

[*Not applicable in this Policy*]

4.9.16 Limits on Suspension Period

[*Not applicable in this Policy*]

4.10 CERTIFICATE STATUS SERVICES

4.10.1 Operational Characteristics

[*Not applicable in this Policy*]

4.10.2 Service Availability

(A) In circumstances in which:

(i) an up to date version of the Organisation ARL has not been lodged in the SMKI Repository in accordance with Part 4.9.7(A) of this Policy; or

(ii) the SMKI Repository Service is unavailable,

a Relying Party shall be entitled to rely on the Organisation ARL for the period during which it remains valid in accordance with the provisions of Part 4.9.7(B) of this Policy, but thereafter shall not rely on any Organisation Certificate or any OCA Certificate.

(B) In circumstances in which:

(i) an up to date version of the Organisation CRL has not been lodged in the SMKI Repository in accordance with Part 4.9.7(C) of this Policy;

or

(ii) the SMKI Repository Service is unavailable,

a Relying Party shall be entitled to rely on the Organisation CRL for the period during which it remains valid in accordance with the provisions of Part 4.9.7(D) of this Policy, but thereafter shall not rely on any Organisation Certificate.

4.10.3 Optional Features

[*Not applicable in this Policy*]

4.11 END OF SUBSCRIPTION

[*Not applicable in this Policy*]

4.12 KEY ESCROW AND RECOVERY

4.12.1 Key Escrow and Recovery Policies and Practices

(A) This Policy does not support Key Escrow.

(B) The OCA shall not provide any Key Escrow service.

4.12.2 Session Key Encapsulation and Recovery Policy and Practices

[*Not applicable in this Policy*]

5 FACILITY, MANAGEMENT AND OPERATIONAL CONTROLS

5.1 PHYSICAL CONTROLS

5.1.1 Site Location and Construction

(A) The OCA shall ensure that the OCA Systems are operated in a sufficiently secure environment, which shall at least satisfy the requirements set out at Section G2 (System Security: Obligations on the DCC) and Section G5 (Information Security: Obligations on the DCC and Users) of the Code.

(B) The OCA shall ensure that:

(i) all of the physical locations in which the OCA Systems are situated, operated, routed or directly accessed are in the United Kingdom;

(ii) all bespoke Security Related Functionality is developed, specified, designed, built and tested only within the United Kingdom; and

(iii) all Security Related Functionality is integrated, configured, tested in situ, implemented, operated and maintained only within the United Kingdom.

(C) The OCA shall ensure that the OCA Systems cannot be indirectly accessed from any location outside the United Kingdom.

(D) The OCA shall ensure that the Organisation CPS incorporates provisions designed to ensure that all physical locations in which the manufacture of Certificates and Time-Stamping take place are at all times manually or electronically monitored for unauthorised intrusion in accordance with the SMKI PMA Guidance on "Protective Monitoring" published on the Website.

(E) The OCA shall ensure that the Organisation CPS incorporates provisions designed to ensure that all PINs, passphrases and passwords used for the purposes of carrying out the functions of the OCA are stored in secure containers accessible only to appropriately authorised individuals.

(F) The OCA shall ensure that the OCA Systems are Separated from any DCA

Systems, save that any Systems used for the purposes of the Registration Authority functions of the OCA and DCA shall not require to be Separated.

5.1.2 Physical Access

(A) The OCA shall ensure that the Organisation CPS incorporates provisions in relation to access control, including in particular provisions designed to:

(i) establish controls such that only appropriately authorised personnel may have unescorted physical access to OCA Systems or any System used for the purposes of Time-Stamping;

(ii) ensure that any unauthorised personnel may have physical access to such Systems only if appropriately authorised and supervised;

(iii) ensure that a site access log is both maintained and periodically inspected for all locations at which such Systems are sited; and

(iv) ensure that all removable media which contain sensitive plain text Data and are kept at such locations are stored in secure containers accessible only to appropriately authorised individuals.

5.1.3 Power and Air Conditioning

(A) The OCA shall ensure that the Organisation CPS incorporates provisions in relation to power and air conditioning at all physical locations in which the OCA Systems are situated.

5.1.4 Water Exposure

(A) The OCA shall ensure that the Organisation CPS incorporates provisions in relation to water exposure at all physical locations in which the OCA Systems are situated.

5.1.5 Fire Prevention and Protection

(A) The OCA shall ensure that the Organisation CPS incorporates provisions in relation to fire prevention and protection at all physical locations in which the OCA Systems are situated.

5.1.6 Media Storage

(A) The OCA shall ensure that the Organisation CPS incorporates provisions designed to ensure that appropriate controls are placed on all media used for the storage of Data held by it for the purposes of carrying out its functions as the OCA.

5.1.7 Waste Disposal

(A) The OCA shall ensure that all media used to store Data held by it for the purposes of carrying out its functions as the OCA are disposed of only using secure methods of disposal in accordance with https://www.ncsc.gov.uk/guidance/secure-sanitisation-storage-media.

5.1.8 Off-Site Back-Up

(A) The OCA shall regularly carry out a Back-Up of:

(i) all Data held on the OCA Systems which are critical to the operation of those Systems or continuity in the provision of the SMKI Services; and

(ii) all other sensitive Data.

(B) For the purposes of paragraph (A), the OCA shall ensure that the Organisation CPS incorporates provisions which identify the categories of critical and sensitive Data that are to be Backed-Up.

(C) The OCA shall ensure that Data which are Backed-Up in accordance with paragraph (A):

(i) are stored on media that are located in physically secure facilities in different locations to the sites at which the Data being Backed-Up are ordinarily held;

(ii) are protected in accordance with the outcome of a risk assessment which is documented in the Organisation CPS, including when being transmitted for the purposes of Back-Up; and

(iii) to the extent to which they comprise OCA Private Key Material, are Backed-Up:

(a) using the proprietary Back-Up mechanisms specific to the relevant Cryptographic Module; and

(b) in a manner that is compliant with FIPS 140-2 Level 3 (or any equivalent to that Federal Information Processing Standard which updates or replaces it from time to time).

(D) The OCA shall ensure that, where any elements of the OCA Systems, any Data held for the purposes of providing the SMKI Services, or any items of OCA equipment are removed from their primary location, they continue to be protected in accordance with the security standard appropriate to the primary location.

5.2 PROCEDURAL CONTROLS

5.2.1 Trusted Roles

(A) The OCA shall ensure that:

(i) no individual may carry out any activity which involves access to resources, or Data held on, the OCA Systems unless that individual has been expressly authorised to have such access;

(ii) each member of OCA Personnel has a clearly defined level of access to the OCA Systems and the premises in which they are located;

(iii) no individual member of OCA Personnel is capable, by acting alone, of engaging in any action by means of which the OCA Systems may be Compromised to a material extent; and

(iv) the Organisation CPS incorporates provisions designed to ensure that appropriate controls are in place for the purposes of compliance by the OCA with the requirements of this paragraph.

5.2.2 Number of Persons Required per Task

(A) The OCA shall ensure that the Organisation CPS incorporates provisions designed to establish:

(i) the appropriate separation of roles between the different members of OCA Personnel; and

(ii) the application of controls to the actions of all members of OCA Personnel who are Privileged Persons, in particular:

(a) identifying any controls designed to ensure that the involvement of more than one individual is required for the performance of certain functions; and

(b) providing that the revocation of any OCA Certificate is one such function.

(B) The OCA shall ensure that the Organisation CPS, as a minimum, makes provision for the purposes of paragraph (A) in relation to the following roles:

(i) OCA Systems administration;

(ii) OCA Systems operations;

(iii) OCA Systems security; and

(iv) OCA Systems auditing.

5.2.3 Identification and Authentication for Each Role

See Part 5.2.2 of this Policy.

5.2.4 Roles Requiring Separation of Duties

See Part 5.2.2 of this Policy.

5.3 PERSONNEL CONTROLS

5.3.1 Qualification, Experience and Clearance Requirements

(A) The OCA shall ensure that all OCA Personnel must:

(i) be appointed to their roles in writing;

(ii) be bound by contract to the terms and conditions relevant to their roles;

(iii) have received appropriate training with respect to their duties;

(iv) be bound by contract not to disclose any confidential, sensitive, personal or security-related Data except to the extent necessary for the performance of their duties or for the purposes of complying with any requirement of law; and

(v) in so far as can reasonably be ascertained by the OCA, not have been previously relieved of any past assignment (whether for the OCA or any other person) on the grounds of negligence or any other failure to perform a duty.

(B) The OCA shall ensure that all OCA Personnel have, as a minimum, passed a Security Check before commencing their roles.

5.3.2 Background Check Procedures

See Part 5.3.1 of this Policy.

5.3.3 Training Requirements

See Part 5.3.1 of this Policy.

5.3.4 Retraining Frequency and Requirements

(A) The OCA shall ensure that the Organisation CPS incorporates appropriate provisions relating to the frequency and content of retraining and refresher training to be undertaken by members of OCA Personnel.

5.3.5 Job Rotation Frequency and Sequence

(A) The OCA shall ensure that the Organisation CPS incorporates appropriate provisions relating to the frequency and sequence of job rotations to be undertaken by members of OCA Personnel.

5.3.6 Sanctions for Unauthorised Actions

(A) The OCA shall ensure that the Organisation CPS incorporates appropriate provisions relating to sanctions for unauthorised actions undertaken by members of OCA Personnel.

5.3.7 Independent Contractor Requirements

(A) In accordance with the provisions of the Code, references to the OCA in this Policy include references to persons with whom the OCA contracts in order to secure performance of its obligations as the OCA.

5.3.8 Documentation Supplied to Personnel

(A) The OCA shall ensure that all OCA Personnel are provided with access to all documents relevant to their roles or necessary for the performance of their duties, including in particular:

(i) this Policy;

(ii) the Organisation CPS; and

(iii) any supporting documentation, statutes, policies or contracts.

5.4 AUDIT LOGGING PROCEDURES

5.4.1 Types of Events Recorded

(A) The OCA shall ensure that:

(i) the OCA Systems record all systems activity in an audit log;

(ii) the Organisation CPS incorporates a comprehensive list of all events that are to be recorded in an audit log in relation to:

(a) the activities of OCA Personnel;

(b) the use of OCA equipment;

(c) the use of (including both authorised and unauthorised access, and attempted access to) any premises at which functions of the OCA are carried out;

(d) communications and activities that are related to the Issue of Certificates (in so far as not captured by the OCA Systems audit log); and

(iii) it records in an audit log all the events specified in paragraph (ii).

5.4.2 Frequency of Processing Log

(A) The OCA shall ensure that:

(i) the audit logging functionality in the OCA Systems is fully enabled at all times;

(ii) all OCA Systems activity recorded in the Audit Log is recorded in a standard format that is compliant with:

(a) British Standard BS 10008:2014 (Evidential Weight and Legal Admissibility of Electronic Information); or

(b) any equivalent to that British Standard which updates or replaces it from time to time; and

(iii) it monitors the OCA Systems in compliance with the SMKI PMA Guidance on “Protective Monitoring” published on the Website.

(B) The OCA shall ensure that the Organisation CPS incorporates provisions which specify:

(i) how regularly information recorded in the Audit Log is to be reviewed; and

(ii) what actions are to be taken by it in response to types of events recorded in the Audit Log.

(C) The OCA shall ensure that the Organisation CPS incorporates provisions in relation to access to the Audit Log, providing in particular that:

(i) Data contained in the Audit Log must not be accessible other than on a read-only basis; and

(ii) access to those Data must be limited to those members of OCA Personnel who are performing a dedicated system audit role.

5.4.3 Retention Period for Audit Log

(A) The OCA shall:

(i) retain the Audit Log so that it incorporates, on any given date, a record of all system events occurring during a period of at least twelve months prior to that date; and

(ii) ensure that a copy of the Audit Log incorporating a record of all system events occurring prior to the beginning of that period is archived in accordance with the requirements of Part 5.5 of this Policy.

5.4.4 Protection of Audit Log

(A) The OCA shall ensure that:

(i) to the extent to which the Audit Log is retained electronically, the Data stored in it cannot be accessed other than on a read-only basis, and are protected from unauthorised viewing, modification and deletion in accordance with:

(a) British Standard BS 10008:2014 (Evidential Weight and Legal Admissibility of Electronic Information); or

(b) any equivalent to that British Standard which updates or replaces it from time to time; and

(ii) to the extent to which the Audit Log is retained in non-electronic form, the Data stored in it are appropriately protected from unauthorised viewing, modification and destruction in order to ensure that their integrity is maintained for evidential purposes.

5.4.5 Audit Log Back-Up Procedures

(A) The OCA shall ensure that the Data contained in the Audit Log are Backed-Up (or, to the extent that the Audit Log is retained in non-electronic form, are copied):

(i) on a daily basis; or

(ii) if activity has taken place on the OCA Systems only infrequently, in accordance with the schedule for the regular Back-Up of the Data held on those Systems.

(B) The OCA shall ensure that all Data contained in the Audit Log which are Backed-Up are, during Back-Up:

(i) held in accordance with the outcome of a risk assessment which is documented in the Organisation CPS; and

(ii) protected to the same standard of protection as the primary copy of the Audit Log in accordance with Part 5.4.4 of this Policy.

5.4.6 Audit Collection System (Internal or External)

(A) The OCA shall ensure that the Organisation CPS incorporates provisions in relation to its system for collecting Data for the purpose of populating the Audit Log.

5.4.7 Notification to Event-Causing Subject

(A) The OCA shall ensure that the Organisation CPS incorporates provisions in relation to its notification of any person who is (or is responsible for any System which is) the direct cause of an event recorded in the Audit Log.

5.4.8 Vulnerability Assessments

(A) Provision is made in Sections G2.13 to G2.14 of the Code (Management of Vulnerabilities) in relation to the carrying out of vulnerability assessments in respect of the OCA Systems.

5.5 RECORDS ARCHIVAL

5.5.1 Types of Records Archived

(A) The OCA shall ensure that it archives:

(i) the Audit Log in accordance with Part 5.4.3 of this Policy;

(ii) its records of all Data submitted to it by Eligible Subscribers for the purposes of Certificate Signing Requests; and

(iii) any other Data specified in this Policy or the Code as requiring to be archived in accordance with this Part 5.5.

5.5.2 Retention Period for Archive

(A) The OCA shall ensure that all Data which are Archived are retained for a period of at least seven years from the date on which they were Archived.

5.5.3 Protection of Archive

(A) The OCA shall ensure that Data held in its Archive are:

(i) protected against any unauthorised access;

(ii) adequately protected against environmental threats such as temperature, humidity and magnetism; and

(iii) incapable of being modified or deleted.

5.5.4 Archive Back-Up Procedures

(A) The OCA shall ensure that the Organisation CPS incorporates provisions in relation to its procedures for the Back-Up of its Archive.

5.5.5 Requirements for Time-Stamping of Records

(A) Provision in relation to Time-Stamping is made in Part 6.8 of this Policy.

5.5.6 Archive Collection System (Internal or External)

(A) The OCA shall ensure that the Organisation CPS incorporates provisions in relation to its system for collecting Data for the purpose of populating the

Archive.

5.5.7 Procedures to Obtain and Verify Archive Information

(A) The OCA shall ensure that:

(i) Data held in the Archive are stored in a readable format during their retention period; and

(ii) those Data remains accessible at all times during their retention period, including during any period of interruption, suspension or cessation of the OCA's operations.

(B) The OCA shall ensure that the Organisation CPS incorporates provisions in relation to the periodic verification by the OCA of the Data held in the Archive.

5.6 KEY CHANGEOVER

5.6.1 Organisation Certificate Key Changeover

(A) The OCA shall Issue a new Organisation Certificate in relation to an Organisation where a new Certificate Signing Request is submitted by an Eligible Subscriber in accordance with the requirements of the SMKI IDS sections 2.3.1.1 to 2.3.1.4 and 2.6.1.1 to 2.6.1.4and this Policy.

5.6.2 OCA Key Changeover

(A) Where the OCA ceases to use an OCA Private Key in accordance with the requirements of Part 4.3.1(E) of this Policy, it shall:

(i) either:

(a) verifiably destroy the OCA Private Key Material; or

(b) retain the OCA Private Key Material in such a manner that it is adequately protected against being put back into use;

(ii) not revoke the related OCA Public Key (which may continue to be used for the purpose of validating Digital Signatures generated using the OCA Private Key);

(iii) generate a new Key Pair;

(iv) ensure that any relevant Certificate subsequently Issued by it is Issued using the OCA Private Key from the newly-generated Key Pair:

(a) until the time determined in accordance with Part 4.3.1(E) of this Policy; and

(b) subject to the provisions of Part 5.7.1(C) of this Policy; and

(v) in its capacity as the Root OCA:

(a) Issue a new relevant OCA Certificate; and

(b) promptly lodge that OCA Certificate in the SMKI Repository.

(B) The OCA shall ensure that the actions taken by it in accordance with the requirements of paragraph (A) are managed so as to prevent any disruption to the provision of the SMKI Services.

5.6.3 Subscriber Key Changeover

(A) Where:

(i) a Certificate has been revoked in accordance with Part 4.9 of this Policy; and

(ii) the Subscriber for that Certificate submits to the OCA a Certificate Signing Request for the Issue of a replacement Certificate,

the OCA shall verify that the reasons for the revocation and replacement of the previous Certificate have been satisfactorily addressed, and may Issue a Certificate in accordance with the Certificate Signing Request only after it has done so.

5.7 COMPROMISE AND DISASTER RECOVERY

5.7.1 Incident and Compromise Handling Procedures

(A) The OCA shall ensure that the Organisation CPS incorporates a business continuity plan which shall be designed to ensure:

(i) continuity in, or (where there has been unavoidable discontinuity) the recovery of, the provision of the SMKI Services in the event of any Compromise of the OCA Systems or major failure in the OCA processes; and

(ii) that priority is given to maintain continuity in, or to recovering the capacity for, the revocation of Certificates and the making available of an up to date Organisation ARL and Organisation CRL.

(B) The OCA shall ensure that the procedures set out in the business continuity plan are:

(i) compliant with ISO 22301 and ISO 27031 (or any equivalent to those standards which update or replace them from time to time); and

(ii) tested periodically, and in any event at least once in each year, in order to ensure that they are operationally effective.

(C) The OCA shall ensure that the Organisation CPS incorporates provisions setting out the approach to be taken by it in circumstances in which it suspects (or has reason to suspect) that any OCA Private Key or any part of the OCA Systems is Compromised.

5.7.2 Computing Resources, Software and/or Data are Corrupted

(A) The OCA shall ensure that the business continuity plan established in accordance with Part 5.7.1 of this Policy incorporates provisions setting out the steps to be taken in the event of any loss of or corruption to computing resources, software or Data.

5.7.3 Entity Private Key Compromise Procedures

See Part 5.7.1 of this Policy.

5.7.4 Business Continuity Capabilities after a Disaster

(A) The OCA shall ensure that the business continuity plan established in accordance with Part 5.7.1 of this Policy is designed to ensure the recovery of the provision of the SMKI Services within not more than 12 hours of the occurrence of any event causing discontinuity.

5.8 CERTIFICATION AUTHORITY AND REGISTRATION AUTHORITY TERMINATION

[*Not applicable in this Policy*]

6 <u>TECHNICAL SECURITY CONTROLS</u>

The OCA shall ensure that the Organisation CPS incorporates detailed provision in relation to the technical controls to be established and operated for the purposes of the exercise of its functions as the Root OCA, the Issuing OCA and the Registration Authority.

6.1 KEY PAIR GENERATION AND INSTALLATION

6.1.1 Key Pair Generation

(A) The OCA shall ensure that all Key Pairs which it uses for the purposes of this Policy are generated:

(i) in a protected environment compliant with FIPS 140-2 Level 3 (or any equivalent to that Federal Information Processing Standard which updates or replaces it from time to time);

(ii) using multi-person control, such that no single Privileged Person is capable of generating any such Key Pair; and

(iii) using random numbers which are such as to make it computationally infeasible to regenerate those Key Pairs even with knowledge of when and by means of what equipment they were generated.

(B) The OCA shall not generate any Private Key or Public Key other than an OCA Key.

6.1.2 Private Key Delivery to Subscriber

(A) In accordance with Part 6.1.1(B), the OCA shall not generate any Private Key for delivery to a Subscriber.

6.1.3 Public Key Delivery to Certificate Issuer

(A) The OCA shall ensure that the Organisation CPS incorporates provisions:

(i) in relation to the mechanism by which Public Keys of Subscribers are delivered to it for the purpose of the exercise of its functions as the

Root OCA and Issuing OCA; and

(ii) ensuring that the mechanism uses a recognised standard protocol such as PKCS#10.

6.1.4 OCA Public Key Delivery to Relying Parties

(A) The OCA shall ensure that the Organisation CPS incorporates provisions:

(i) in relation to the manner by which each OCA Public Key is to be lodged in the SMKI Repository; and

(ii) designed to ensure that the OCA Public Keys are securely lodged in the SMKI Repository in such a manner as to guarantee that their integrity is maintained.

6.1.5 Key Sizes

(A) The OCA and every Subscriber shall ensure that all Private Keys and Public Keys which each of them may use for the purposes of this Policy are of the size and characteristics set out in the GB Companion Specification.

6.1.6 Public Key Parameters Generation and Quality Checking

(A) The OCA shall ensure that any Public Key used by it for the purposes of this Policy shall be of values and lengths that make the success of known attacks infeasible.

(B) Each Subscriber shall ensure that any Public Key used by it for the purposes of this Policy shall be of values and lengths that make the success of known attacks infeasible.

6.1.7 Key Usage Purposes (as per X.509 v3 `keyUsage` Field)

(A) The OCA shall ensure that each Certificate that is Issued by it has a `keyUsage` field in accordance with RFC5759 and RFC5280.

(B) The OCA shall ensure that each Organisation Certificate that is Issued by it has a `keyUsage` of either:

(i) `digitalSignature`; or

(ii) `keyAgreement`.

(C) The OCA shall ensure that each OCA Certificate that is Issued by it has a `keyUsage` of either:

(i) `keyCertSign`; or

(ii) `CRLSign`.

(D) The OCA shall ensure that no `keyUsage` values may be set in an Organisation Certificate or OCA Certificate other than in accordance with this Part 6.1.7.

6.2 PRIVATE KEY PROTECTION AND CRYPTOGRAPHIC MODULE ENGINEERING CONTROLS

6.2.1 Cryptographic Module Standards and Controls

(A) The OCA shall ensure that all OCA Private Keys shall be:

(i) protected to a high standard of assurance by physical and logical security controls; and

(ii) stored in and operated from within a Cryptographic Module which is compliant with FIPS 140-2 Level 3 (or any equivalent to that Federal Information Processing Standard which updates or replaces it from time to time).

(B) The OCA shall ensure that all OCA Private Keys shall, where they affect the outcome of any Certificates Issued by it, be protected by, stored in and operated from within a Cryptographic Module which is compliant with FIPS 140-2 Level 3 (or any equivalent to that Federal Information Processing Standard which updates or replaces it from time to time).

(C) The OCA shall ensure that no OCA Private Key shall be made available in either complete or unencrypted form except in a Cryptographic Module which is compliant with FIPS 140-2 Level 3 (or any equivalent to that Federal Information Processing Standard which updates or replaces it from time to time).

(D) The OCA shall ensure that any Cryptographic Module which is used for any purpose related to Certificate life-cycle management shall:

(i) operate so as to block access to itself following a number of failed consecutive attempts to access it using Activation Data, where that number shall be set out in the Organisation CPS; and

(ii) be required to be unblocked by an authorised member of OCA Personnel who has been Authenticated as such following a process which shall be set out in the Organisation CPS.

6.2.2 Private Key (m out of n) Multi-Person Control

See Part 6.1.1 of this Policy.

6.2.3 Private Key Escrow

(A) This Policy does not support Key Escrow.

(B) The OCA shall not provide any Key Escrow service.

6.2.4 Private Key Back-Up

(A) The OCA may Back-Up OCA Private Keys insofar as:

(i) each Private Key is protected to a standard which is at least equivalent to that required in relation to the principal Private Key in accordance with this Policy; and

(ii) where more than one Private Key is Backed-Up within a single security environment, each of the Private Keys which is Backed-Up within that environment must be protected to a standard which is at least equivalent to that required in relation to an Issuing OCA Private Key in accordance with this Policy.

6.2.5 Private Key Archival

(A) The OCA shall ensure that no OCA Key which is a Private Key is archived.

6.2.6 Private Key Transfer into or from a Cryptographic Module

(A) The OCA shall ensure that no OCA Private Key is transferred or copied other than:

(i) for the purposes of:

(a) Back-Up;

(b) establishing an appropriate degree of resilience in relation to the provision of the SMKI Services; or

(c) in other circumstances where the SMKI PMA has (following consultation with the Security Sub-Committee) given explicit approval to do so in order to maintain continuity of the provision of SMKI Services.

(ii) in accordance with a level of protection which is compliant with FIPS 140-2 Level 3 (or any equivalent to that Federal Information Processing Standard which updates or replaces it from time to time).

6.2.7 Private Key Storage on Cryptographic Module

See Part 6.2.1 of this Policy.

6.2.8 Method of Activating Private Key

(A) The OCA shall ensure that the Cryptographic Module in which any OCA Private Key is stored may be accessed only by an authorised member of OCA Personnel who has been Authenticated following an Authentication process which:

(i) has an appropriate level of strength to ensure the protection of the Private Key; and

(ii) involves the use of Activation Data.

6.2.9 Method of Deactivating Private Key

(A) The OCA shall ensure that any OCA Private Key shall be capable of being de-activated by means of the OCA Systems, at least by:

(i) the actions of:

(a) turning off the power;

(b) logging off;

(c) carrying out a system reset; and

(ii) a period of inactivity of a length which shall be set out in the Organisation CPS.

6.2.10 Method of Destroying Private Key

(A) The OCA shall ensure that the Organisation CPS incorporates provisions for the exercise of strict controls in relation to the destruction of OCA Keys.

(B) The OCA shall ensure that no OCA Key (whether in active use, existing as a copy for the purposes of resilience, or Backed-Up) is destroyed except in accordance with a positive decision by the OCA to destroy it.

6.2.11 Cryptographic Module Rating

See Part 6.2.1 of this Policy.

6.3 OTHER ASPECTS OF KEY PAIR MANAGEMENT

6.3.1 Public Key Archival

(A) The OCA shall ensure that it archives OCA Public Keys in accordance with the requirements of Part 5.5 of this Policy.

6.3.2 Certificate Operational Periods and Key Pair Usage Periods

(A) The OCA shall ensure that the Validity Period of each Certificate Issued by it shall be as follows:

(i) in the case of an Organisation Certificate, 10 years or, a different duration in circumstances approved by the SMKI PMA (having taken into account the views of the Security Sub-Committee;

(ii) in the case of an Issuing OCA Certificate, 25 years; and

(iii) in the case of a Root OCA Certificate, 50 years.

(B) For the purposes of paragraph (A), the OCA shall set the `notAfter` value specified in Annex B in accordance with that paragraph.

(C) The OCA shall ensure that no OCA Private Key is used after the end of the Validity Period of the Certificate containing the Public Key which is associated with that Private Key.

6.4 ACTIVATION DATA

6.4.1 Activation Data Generation and Installation

(A) The OCA shall ensure that any Cryptographic Module within which an OCA Key is held has Activation Data that are unique and unpredictable.

(B) The OCA shall ensure that:

(i) these Activation Data, in conjunction with any other access control, shall be of an appropriate level of strength for the purposes of protecting the OCA Keys; and

(ii) where the Activation Data comprise any PINs, passwords or pass-phrases, the OCA shall have the ability to change these at any time.

6.4.2 Activation Data Protection

(A) The OCA shall ensure that the Organisation CPS incorporates provision for the use of such cryptographic protections and access controls as are appropriate to protect against the unauthorised use of Activation Data.

6.4.3 Other Aspects of Activation Data

[*Not applicable in this Policy*]

6.5 COMPUTER SECURITY CONTROLS

6.5.1 Specific Computer Security Technical Requirements

(A) The OCA shall ensure that the Organisation CPS incorporates provisions in relation to the identification and implementation, following the conclusion of any threat assessment, of security measures which make provision for at least the following:

(i) the establishment of access controls in relation to the activities of the OCA;

(ii) the appropriate allocation of responsibilities to Privileged Persons;

(iii) the identification and Authentication of organisations, individuals and Systems involved in OCA activities;

(iv) the use of cryptography for communication and the protection of Data stored on the OCA Systems;

(v) the audit of security related events; and

(vi) the use of recovery mechanisms for OCA Keys.

6.5.2 Computer Security Rating

(A) The OCA shall ensure that the Organisation CPS incorporates provisions relating to the appropriate security rating of the OCA Systems.

6.6 LIFE-CYCLE TECHNICAL CONTROLS

6.6.1 System Development Controls

(A) The OCA shall ensure that any software which is developed for the purpose of establishing a functionality of the OCA Systems shall:

(i) take place in a controlled environment that is sufficient to protect against the insertion into the software of malicious code;

(ii) be undertaken by a developer which has a quality system that is:

(a) compliant with recognised international standards (such as ISO 9001:2000 or an equivalent standard); or

(b) available for inspection and approval by the SMKI PMA, and has been so inspected and approved.

6.6.2 Security Management Controls

(A) The OCA shall ensure that the Organisation CPS incorporates provisions which are designed to ensure that the OCA Systems satisfy the requirements of Section G2 (System Security: Obligations on the DCC) and Section G5 (Information Security: Obligations on the DCC and Users) of the Code.

6.6.3 Life-Cycle Security Controls

See Part 6.6.2 of this Policy.

6.7 NETWORK SECURITY CONTROLS

6.7.1 Use of Offline Root OCA

(A) The OCA shall ensure that its functions as the Root OCA are carried out on a part of the OCA Systems that is neither directly nor indirectly connected to any System which is not a part of the OCA Systems.

6.7.2 Protection Against Attack

(A) The OCA shall use its best endeavours to ensure that the OCA Systems are not Compromised, and in particular for this purpose that they are designed and operated so as to detect and prevent:

(i) any Denial of Service Event; and

(ii) any unauthorised attempt to connect to them.

(B) The OCA shall take reasonable steps to ensure that the OCA Systems cause or permit to be open at any time only those network ports, and allow only those protocols, which are required at that time for the effective operation of those Systems, and block all network ports and protocols which are not so required.

6.7.3 Separation of Issuing OCA

(A) The DCC shall ensure that, where its functions as the Issuing OCA are carried out on a part of the OCA Systems that is connected to an external network, they are carried out on a System that is Separated from all other OCA Systems.

6.7.4 Health Check of OCA Systems

(A) The OCA shall ensure that, in relation to the OCA Systems, a vulnerability assessment in accordance with Section G2.13 – G2.15 of the Code (Management of Vulnerabilities) is carried out with such frequency as may be specified from time to time by the Independent SMKI Assurance Service Provider.

6.8 TIME-STAMPING

6.8.1 Use of Time-Stamping

(A) The OCA shall ensure that Time-Stamping takes place in relation to all Certificates and all other OCA activities which require an accurate record of time.

(B) The OCA shall ensure that the Organisation CA incorporates provisions in relation to the time source and mechanisms used by any Time-Stamping Authority which carries out Time-Stamping on behalf of the OCA.

7 <u>CERTIFICATE, CRL AND OCSP PROFILES</u>

7.1 CERTIFICATE PROFILES

(A) The OCA shall use only the Certificate Profiles in Annex B.

7.1.1 Version Number(s)

[*Not applicable in this Policy*]

7.1.2 Certificate Extensions

[*Not applicable in this Policy*]

7.1.3 Algorithm Object Identifiers

[*Not applicable in this Policy*]

7.1.4 Name Forms

[*Not applicable in this Policy*]

7.1.5 Name Constraints

[*Not applicable in this Policy*]

7.1.6 Certificate Policy Object Identifier

[*Not applicable in this Policy*]

7.1.7 Usage of Policy Constraints Extension

[*Not applicable in this Policy*]

7.1.8 Policy Qualifiers Syntax and Semantics

[*Not applicable in this Policy*]

7.1.9 Processing Semantics for the Critical Certificate Policies Extension

[*Not applicable in this Policy*]

7.2 CRL PROFILE

7.2.1 Version Number(s)

(A) The OCA shall ensure that the Organisation ARL and Organisation CRL conform with X.509 v2 and IETF RFC 5280.

7.2.2 CRL and CRL Entry Extensions

(A) The OCA shall notify Parties of the profile of the Organisation CRL and of any Organisation CRL extensions.

7.3 OCSP PROFILE

7.3.1 Version Number(s)

[*Not applicable in this Policy*]

7.3.2 OCSP Extensions

[*Not applicable in this Policy*]

8 COMPLIANCE AUDIT AND OTHER ASSESSMENTS

8.1 FREQUENCY OR CIRCUMSTANCES OF ASSESSMENT

(A) Provision in relation to this is made in Appendix C of the Code (SMKI Compliance Policy).

8.2 IDENTITY/QUALIFICATIONS OF ASSESSOR

(A) Provision in relation to this is made in Appendix C of the Code (SMKI Compliance Policy).

8.3 ASSESSOR'S RELATIONSHIP TO ASSESSED ENTITY

(A) Provision in relation to this is made in Appendix C of the Code (SMKI Compliance Policy).

8.4 TOPICS COVERED BY ASSESSMENT

(A) Provision in relation to this is made in Appendix C of the Code (SMKI Compliance Policy).

8.5 ACTIONS TAKEN AS A RESULT OF DEFICIENCY

(A) Provision in relation to this is made in Appendix C of the Code (SMKI Compliance Policy).

8.6 COMMUNICATION OF RESULTS

(A) Provision in relation to this is made in Appendix C of the Code (SMKI Compliance Policy).

9 OTHER BUSINESS AND LEGAL MATTERS

In so far as provision is made in relation to all the matters referred to in this Part, it is found in the DCC Licence and the provisions of the Code (including in Section L11 (Subscriber Obligations) and Section L12 (Relying Party Obligations) of the Code).

9.1 FEES

(A) See the statement at the beginning of this Part.

9.1.1 Certificate Issuance or Renewal Fees

(A) See the statement at the beginning of this Part.

9.1.2 Organisation Certificate Access Fees

(A) See the statement at the beginning of this Part.

9.1.3 Revocation or Status Information Access Fees

(A) See the statement at the beginning of this Part.

9.1.4 Fees for Other Services

(A) See the statement at the beginning of this Part.

9.1.5 Refund Policy

(A) See the statement at the beginning of this Part.

9.2 FINANCIAL RESPONSIBILITY

9.2.1 Insurance Coverage

(A) See the statement at the beginning of this Part.

9.2.2 Other Assets

(A) See the statement at the beginning of this Part.

9.2.3 Insurance or Warranty Coverage for Subscribers and Subjects

(A) See the statement at the beginning of this Part.

9.3 CONFIDENTIALITY OF BUSINESS INFORMATION

9.3.1 Scope of Confidential Information

(A) See the statement at the beginning of this Part.

9.3.2 Information not within the Scope of Confidential Information

(A) See the statement at the beginning of this Part.

9.3.3 Responsibility to Protect Confidential Information

(A) See the statement at the beginning of this Part.

9.4 PRIVACY OF PERSONAL INFORMATION

9.4.1 Privacy Plan

(A) See the statement at the beginning of this Part.

9.4.2 Information Treated as Private

(A) See the statement at the beginning of this Part.

9.4.3 Information not Deemed Private

(A) See the statement at the beginning of this Part.

9.4.4 Responsibility to Protect Private Information

(A) See the statement at the beginning of this Part.

9.4.5 Notice and Consent to Use Private Information

(A) See the statement at the beginning of this Part.

9.4.6 Disclosure Pursuant to Judicial or Administrative Process

(A) See the statement at the beginning of this Part.

9.4.7 Other Information Disclosure Circumstances

(A) See the statement at the beginning of this Part.

9.5 INTELLECTUAL PROPERTY RIGHTS

(A) See the statement at the beginning of this Part.

9.6 REPRESENTATIONS AND WARRANTIES

9.6.1 Certification Authority Representations and Warranties

(A) See the statement at the beginning of this Part.

9.6.2 Registration Authority Representations and Warranties

(A) See the statement at the beginning of this Part.

9.6.3 Subscriber Representations and Warranties

(A) See the statement at the beginning of this Part.

9.6.4 Relying Party Representations and Warranties

(A) See the statement at the beginning of this Part.

9.6.5 Representations and Warranties of Other Participants

(A) See the statement at the beginning of this Part.

9.7 DISCLAIMERS OF WARRANTIES

(A) See the statement at the beginning of this Part.

9.8 LIMITATIONS OF LIABILITY

(A) See the statement at the beginning of this Part.

9.9 INDEMNITIES

(A) See the statement at the beginning of this Part.

9.10 TERM AND TERMINATION

9.10.1 Term

(A) See the statement at the beginning of this Part.

9.10.2 Termination of Organisation Certificate Policy

(A) See the statement at the beginning of this Part.

9.10.3 Effect of Termination and Survival

(A) See the statement at the beginning of this Part.

9.11 INDIVIDUAL NOTICES AND COMMUNICATIONS WITH PARTICIPANTS

9.11.1 Subscribers

(A) See the statement at the beginning of this Part.

9.11.2 Organisation Certification Authority

(A) See the statement at the beginning of this Part.

9.11.3 Notification

(A) See the statement at the beginning of this Part.

9.12 AMENDMENTS

9.12.1 Procedure for Amendment

(A) See the statement at the beginning of this Part.

9.12.2 Notification Mechanism and Period

(A) See the statement at the beginning of this Part.

9.12.3 Circumstances under which OID Must be Changed

(A) See the statement at the beginning of this Part.

9.13 DISPUTE RESOLUTION PROVISIONS

(A) See the statement at the beginning of this Part.

9.14 GOVERNING LAW

(A) See the statement at the beginning of this Part.

9.15 COMPLIANCE WITH APPLICABLE LAW

(A) See the statement at the beginning of this Part.

9.16 MISCELLANEOUS PROVISIONS

9.16.1 Entire Agreement

(A) See the statement at the beginning of this Part.

9.16.2 Assignment

(A) See the statement at the beginning of this Part.

9.16.3 Severability

(A) See the statement at the beginning of this Part.

9.16.4 Enforcement (Attorney’s Fees and Waiver of Rights)

(A) See the statement at the beginning of this Part.

9.16.5 Force Majeure

(A) See the statement at the beginning of this Part.

9.17 OTHER PROVISIONS

9.17.1 Organisation Certificate Policy Content

(A) See the statement at the beginning of this Part.

9.17.2 Third Party Rights

(A) See the statement at the beginning of this Part.

ANNEX A: DEFINITIONS AND INTERPRETATION

In this Policy, except where the context otherwise requires -

- expressions defined in Section A of the Code (Definitions and Interpretation) have the same meaning as is set out in that Section,
- the expressions in the left-hand column below shall have the meanings given to them in the right-hand column below,
- where any expression is defined in Section A of the Code (Definitions and Interpretation) and in this Annex, the definition in this Annex shall take precedence for the purposes of the Policy,
- the rule of interpretation set out at Part 1.1 of this Policy shall apply.

Activation Data means any private Data (such as a password or the Data on a smartcard) which are used to access a Cryptographic Module.

Archive means the archive of Data created in accordance with Part 5.5.1 of this Policy (and "**Archives**" and "**Archived**" shall be interpreted accordingly).

Audit Log means the audit log created in accordance with Part 5.4.1 of this Policy.

Authentication means the process of establishing that an individual, Certificate, System or Organisation is what he or it claims to be (and "**Authenticate**" and "**Authenticated**" shall be interpreted accordingly).

Authorised Subscriber means a Party or RDP which has successfully completed the procedures set out in the SMKI RAPP and has been authorised by the OCA to submit a Certificate Signing Request.

Certificate means either an Organisation Certificate or an OCA Certificate.

Certificate Profile means a table bearing that title in Annex B and specifying certain parameters to be contained within a Certificate.

Certificate Re-Key means a change to the Public Key contained within a Certificate bearing a particular serial number.

Certificate Revocation Request means a request for the revocation of a Certificate by the OCA, submitted by the Subscriber for that Certificate to the OCA in accordance with the SMKI RAPP and this Policy.

DCA Systems has the meaning given to that expression in Appendix A of the Code (Device Certificate Policy).

Eligible Subscriber means:

(a) in relation to an Organisation Certificate, an Authorised Subscriber which is identified as an Eligible Subscriber in accordance with Section L3.18 of the Code (Organisation Certificates); and

(b) in relation to an OCA Certificate, an Authorised Subscriber which is identified as an Eligible Subscriber in accordance with Section L3.19 of the Code (OCA Certificates).

Entity Identifier means a User ID, RDP ID or a DCC ID as required by the context.

Issue means the act of the OCA, in its capacity as the Root OCA or Issuing OCA, and acting in accordance with this Policy, of creating and signing a Certificate which is bound to both a Subject and a Subscriber (and “**Issued**” and “**Issuing**” shall be interpreted accordingly).

Issuing Organisation Certification Authority (or **Issuing OCA**) means the DCC exercising the function of Issuing Organisation Certificates to Eligible Subscribers and of storing and managing the Private Keys associated with that function.

Issuing OCA Certificate means a certificate in the form set out in the Issuing OCA Certificate Profile in accordance with Annex B, and Issued by the Root OCA to the Issuing OCA in accordance with this Policy.

Issuing OCA Private Key means a Private Key which is stored and managed by the OCA acting in its capacity as the Issuing OCA.

Issuing OCA Public Key means the Public Key which is part of a Key Pair with an Issuing OCA Private Key.

Key Escrow means the storage of a Private Key by a person other than the Subscriber or Subject of the Certificate which contains the related Public Key.

Object Identifier (or **OID**) means an Object Identifier assigned by the Internet Address Naming Authority.

OCA Certificate means either a Root OCA Certificate or an Issuing OCA Certificate.

OCA Key means any Private Key or a Public Key generated by the OCA for the purposes of complying with its obligations under the Code.

OCA Personnel means the DCC Personnel working on behalf of the OCA.

OCA Private Key means either a Root OCA Private Key or an Issuing OCA Private Key.

OCA Systems means the Systems used by the OCA in relation to the SMKI Services.

Organisation Authority Revocation List (or **ARL**) means a list, produced by the OCA, of all OCA Certificates that have been revoked in accordance with this Policy.

Organisation Certificate means a certificate in the form set out in the Organisation Certificate Profile in accordance with Annex B, and Issued by the Issuing OCA in accordance with this Policy.

Organisation Certificate Revocation List (or **CRL**) means a list, produced by the OCA, of all Organisation Certificates that have been revoked in accordance with this Policy.

Organisation Certification Authority (or **OCA**) means the DCC, acting in the capacity and exercising the functions of one or more of:

(a) the Root OCA;

(b) the Issuing OCA; and

(c) the Registration Authority.

Private Key Material in relation to a Private Key, means that Private Key and the input parameters necessary to establish, use and maintain it.

Registration Authority means the DCC exercising the function of receiving and processing Certificate Signing Requests made in accordance with the SMKI RAPP.

SMKI Registration Authority Manager has the meaning given to that expression in the SMKI RAPP.

SMKI Registration Authority Personnel has the meaning given to that expression in the SMKI RAPP.

Root Organisation Certification Authority (or **Root OCA**) means the DCC exercising the function of Issuing OCA Certificates to the Issuing OCA and storing and managing Private Keys associated with that function.

Root OCA Certificate means a certificate in the form set out in the Root OCA Certificate Profile in accordance with Annex B and self-signed by the Root OCA in accordance with this Policy.

Root OCA Private Key means a Private Key which is stored and managed by the OCA acting in its capacity as the Root OCA.

Security Related Functionality means the functionality of the OCA Systems which is designed to detect, prevent or mitigate the adverse effect of any Compromise of that System.

Subject means:

(a) in relation to an Organisation Certificate, the Organisation identified by the `subject` field of the Organisation Certificate Profile in Annex B; and

(b) in relation to an OCA Certificate, the globally unique name of the Root OCA or Issuing OCA as identified by the `subject` field of the relevant Certificate Profile in Annex B.

Subscriber means, in relation to any Certificate, a Party or RDP which has been Issued with and accepted that Certificate, acting in its capacity as the holder of the Certificate.

Time-Stamping means the act that takes place when a Time-Stamping Authority, in relation to a Certificate, stamps a particular datum with an accurate indicator of the time (in hours, minutes and seconds) at which the activity of stamping takes place.

Time-Stamping Authority means that part of the OCA that:

(a) where required, provides an appropriately precise time-stamp in the format required by this Policy; and

(b) relies on a time source that is:

(i) accurate;

(ii) determined in a manner that is independent of any other part of the OCA Systems; and

(iii) such that the time of any time-stamp can be verified to be that of the Independent Time Source at the time at which the time-stamp was applied.

Validity Period means, in respect of a Certificate, the period of time for which that Certificate is intended to be valid.

ANNEX B: OCA CERTIFICATE AND ORGANISATION CERTIFICATE PROFILES

End Entity Certificate Structure and Contents

This Annex lays out requirements as to structure and content with which OCA Certificates and Organisation Certificates shall comply. All terms in this Annex shall, where not defined in the Code, this Policy, or the GB Companion Specification, have the meanings in IETF RFC 5759 and IETF RFC5280.

Common requirements applicable to OCA Certificates and Organisation Certificates

All OCA Certificates and Organisation Certificates that are validly authorised within the SMKI for use within the scope of GB Smart Metering:

- shall be compliant with IETF RFC 5759 and so with IETF RFC5280.
- for clarity and in adherence with the requirements of IETF RFC5759, all OCA Certificates and Organisation Certificates shall:
    - contain the `authorityKeyIdentifier` extension, except where the Certificate is the Root OCA Certificate;
    - contain the `keyUsage` extension which shall be marked as critical;
- be X.509 v3 certificates as defined in IETF RFC 5280, encoded using the ASN.1 Distinguished Encoding Rules;
- shall, in relation to communications with devices, contain a non-empty subject field which contains an `X520OrganizationalUnitName` whose value is to be expressed as the human-readable two octet hexadecimal representation of the integer Remote Party Role that the Certificate allows the Subject of the Certificate to perform;
- only contain Public Keys of types that are explicitly allowed by the GBCS. This means all Public Keys shall be elliptic curve Public Keys on the NIST P-256 curve;
- only contain Public Keys in uncompressed form i.e. contain an elliptic curve point in uncompressed form as detailed in Section 2.2 of IETF RFC5480;
- only provide for signature methods that are explicitly allowed within the GBCS. This means using P-256 Private Keys with SHA 256 and ECDSA;

- contain a `certificatePolicies` extension containing at least one `CertPolicyID` which shall be marked as critical. For clarity and in adherence with IETF RFC 5280, Certification Path Validation undertaken by Parties and Devices shall interpret this extension;
- contain a `serialNumber` of no more than 16 octets in length;
- contain a `subjectKeyIdentifier` which shall be marked as non-critical;
- contain an `authorityKeyIdentifier` in the form `[0] KeyIdentifier` which shall be marked as non-critical, except where the Certificate is the Root OCA Certificate. Note this exception only applies where Remote Party Role as specified in the `X520OrganizationalUnitName` part of the `subject` field = root;
- only contain `KeyIdentifiers` generated as per method (2) of Section 4.2.1.2 of IETF RFC 5280 and so which shall always be 8 octets in length;
- contain an `issuer` field whose contents MUST be identical to the contents of the signer's `subject` field in the signer's Certificate;
- have a valid `notBefore` field consisting of the time of issue encoded and a valid `notAfter` field expiration date as per IETF RFC 5280 Section 4.1.2.5.

Requirements applicable to Organisation Certificates only

All Organisation Certificates that are issued by the OCA shall:

- within the `subject` field, in addition to other attributes, contain an `AttributeTypeAndValue` structure whose type shall be `id-at-uniqueIdentifier {joint-iso-itu-t(2) ds(5) attributeType(4) uniqueIdentifier(45)}` and whose value shall be the 8 octet Entity Identifier of the subject of the Certificate;
- contain a single Public Key;
- contain a `keyUsage` extension marked as critical, with a value of only one of:
  - `digitalSignature`; or
  - `keyAgreement`.

- contain a single `CertPolicyID` in the `certificatePolicies` extension that refers to the OID of this Policy under which the Certificate is issued.

Requirements applicable to the Root OCA and Issuing OCA

All OCA Certificates issued by the OCA shall:

- have globally unique `subject` field contents;
- contain a single public key except for the Root-CA where there shall be two public keys. The second public key shall be referred to as the Contingency Key and shall be present in the `WrappedApexContingencyKey` extension with the meaning of IETF RFC5934 section 9. The Contingency Key shall be encrypted as per the requirements of the GBCS;
- contain a `keyUsage` extension marked as critical and defined as:
  - `keyCertSign`; and
  - `cRLSign`;
- for Issuing OCA Certificates, contain at least one `CertPolicyID` in the `certificatePolicies` extension that refers to the OID of this Policy under which the Certificate is issued;
- for the Root OCA Certificate, contain a single `CertPolicyID` in the `certificatePolicies` extension that refers to the OID for `anyPolicy`;
- for Issuing OCA Certificates, contain the `basicConstraints` extension, with values `cA=True`, and `pathLen=0`. This extension shall be marked as critical;
- for the Root OCA Certificate, contain the basicConstraints extension, with the value `cA=True` and `pathLen absent` (unlimited). This extension shall be marked as critical.

Organisation Certificate Profile

Field Name	RFC 5759/5280 Type	Value	Reference
version	INTEGER	v3	
serialNumber	INTEGER	Positive Integer of up to 16 Octets	
signature	AlgorithmIdentifier	SHA256 with ECDSA	
The value field of the AttributeTypeAndValue structure within the subject field whose type is id-at-commonName (the "Issuer X520 Common Name")	UTF8String	Globally unique common name of Issuing OCA of up to 4 Octets (as defined in the Issuing OCA Certificate Profile)	
keyIdentifier in Authoritykeyidentifier (the "Subject Key Identifier")	keyIdentifier	A unique value that matches the subjectKeyIdentifier value of the issuer's credential	
keyIdentifier in subjectKeyIdentifier (the "Subject Key Identifier")	keyIdentifier	Provides a means for identifying certificates containing the particular Public Key used in an application	

notBefore	Time	Creation time of the Organisation Certificate	
notAfter	Time	Expiry time of the Certificate	
The value field of the AttributeTypeAndValue structure within the subject field whose type is id-at-commonName (the “Subject X520 Common Name”)	UTF8String	Name of the Subject of up to 16 Octets	
The value field of the AttributeTypeAndValue structure within the subject field whose type is id-at-organizationalUnitName (the “Subject X520 Organizational Unit Name”)	UTF8String	Remote Party Role of the subject of the Certificate	
The value field of the AttributeTypeAndValue structure within the subject field whose type is id-at-uniqueIdentifier	UniqueIdentifier	The 64 bit Entity Identifier of the subject of the Certificate	

(the “Subject Unique Identifier”)			
`subjectPublicKeyInfo`	`SubjectPublicKeyInfo`	The subject’s Public Key	
`extensions`	`Extensions`	Critical and non-critical extensions	
`signatureAlgorithm`	`AlgorithmIdentifier`	SHA256 with ECDSA	
`signatureValue`	`BIT STRING`	Subject Organisation Certificate signature	

Interpretation

`version`

The version of the X.509 Organisation Certificate. Valid Organisation Certificates shall identify themselves as version 3.

`serialNumber`

Organisation Certificate serial number, a positive integer of up to 16 octets. The `serialNumber` identifies the Organisation Certificate, and shall be created by the Issuing OCA that signs the Organisation Certificate. The `serialNumber` shall be unique in the scope of Organisation Certificate signed by the Issuing OCA.

`signature`

The identity of the signature algorithm used to sign the Organisation Certificate. The field is identical to the value of the Organisation Certificate `signatureAlgorithm` field explained further under the next **`signatureAlgorithm`** heading.

Issuer X520 Common Name

The name of the signer of the Organisation Certificate. This will be the gloablly unique name of the Issuing OCA of up to 4 Octets (as defined in the Issuing OCA Certificate Profile).

Authority Key Identifier

To optimize building the correct credential chain, the non-critical Authority Key Identifier extension shall be populated with a unique value as recommended by RFC 5280 and shall be included in all Organisation Certificates.

Subject Key Identifier

The Subject Key Identifier extension shall be included and marked as non-critical in the Organisation Certificate.

`validity`

The time period over which the Issuing OCA expects the Organisation Certificate to be valid. The `validity` period is the period of time from `notBefore` through `notAfter`, inclusive.

All times shall be stated in the Universal Coordinated Time (UTC) time zone. Times up to and including 23:59:59 December 31, 2049 UTC shall be encoded as `UTCTime` as YYMMDDHHmmssZ.

Times later than 23:59:59 December 31, 2049 UTC shall be encoded as `GeneralizedTime` as YYYYMMDDHHmmssZ.

`notBefore`

The earliest time an Organisation Certificate may be used. This shall be the time the Organisation Certificate is created.

`notAfter`

The latest time an Organisation Certificate is expected to be used. The value in a `notAfter` field shall be treated as specified in RFC 5280.

Subject X520 Common Name

This field shall contain a unique X.500 Distinguished Name (DN).

This field shall only be populated with a value where:

- the value of `keyUsage` within **extensions** is `digitalSignature`; and
- the **Subject X520 Organizational Unit Name** field has a value of either '02' or '87'.

Where this field is populated:

- it shall, where the **Subject X520 Organizational Unit Name** field has a value of '02' (so Supplier with its GBCS meaning), contain the string which the eligible subscriber wishes to have displayed in the Supplier's name field within Contact Details (with its SMETS meaning), should the Certificate be placed on a Smart Meter; and
- it shall, where the **Subject X520 Organizational Unit Name** field has a value of '87' (so corresponding to the Remote Party Role of xmlSign with its Section L meaning):
    - where the Subject Unique Identifier field is to be populated with an identification number that is (or is to be) used by the eligible subscriber acting in the User Role of Import Supplier and/or Gas Supplier and/or Export Supplier, include one or two of the Market Participant Identifiers by which the eligible subscriber may be identified in the Party Details. Where two such identifiers are included, only one shall relate to the supply of gas and one to the supply of electricity, and they shall be separated by a single space character. There shall be no other whitespace characters; or
    - otherwise, be populated with a string chosen by the eligible subscriber.

The field shall be a maximum of 16 characters in length.

Subject X520 Organizational Unit Name

The Subject X520 Organizational Unit Name attribute of `subject` shall be populated with the Remote Party Role Code that the Certificate allows the subject of the Certificate to perform.

Subject Unique Identifier

This shall be populated with the 64-bit Entity Identifier of the subject of the Certificate

`subjectPublicKeyInfo`

The Organisation Certificate `subjectPublicKeyInfo` field shall indicate the Public Key algorithm identifier and the Public Key in the specified algorithm format as specified in RFC 3279 and RFC 5480.

The algorithm field in the `subjectPublicKeyInfo` structure shall contain the following identifier:

```
id-ecPublicKey OBJECT IDENTIFIER ::= {iso(1) member-body(2)
us(840) ansi-X9-62(10045) keyType(2) 1 }
```

`id-ecPublicKey` indicates that the algorithms that can be used with the subject Public Key are unrestricted. The key is only restricted by the values indicated in the `keyUsage` Organisation Certificate extension (explained further under the next **`extensions`** heading).

The parameter for `id-ecPublicKey` is as follows and shall always be present:

```
ECParameters ::= CHOICE {

      namedCurve         OBJECT IDENTIFIER

      -- implicitCurve   NULL

      -- specifiedCurve  SpecifiedECDomain

    }
```

Only the following field in ECParameters shall be used:

- o `namedCurve` - identifies all the required values for a particular set of elliptic curve domain parameters to be represented by an object identifier.

The `OBJECT IDENTIFIER` for the curve choice to be used in Organisation Certificate is:

```
secp256r1 OBJECT IDENTIFIER ::= { iso(1) member-body(2)
us(840) ansi-X9-62(10045) curves(3) prime(1) 7 }
```

The `subjectPublicKey` from `SubjectPublicKeyInfo` is the ECC Public Key.

Implementations of Elliptic Curve Cryptography according to this document shall only support the uncompressed form.

The first octet of the `subjectPublicKey` indicates whether the key is compressed or uncompressed. The uncompressed form is indicated by 0x04 (the compressed form is indicated by either 0x02 or 0x03). The Public Key shall be rejected if any value other than 0x04 is in the first octet.

`signatureAlgorithm`

The `signatureAlgorithm` field shall indicate the Issuing OCA signature algorithm used to sign this Organisation Certificate is as defined under the next **Signature Method (ECDSA)** heading.

`signatureValue`

The Issuing OCA's signature of the Organisation Certificate shall be computed using the Issuing OCA's private signing key using the algorithm identified under the next **Signature Method (ECDSA)** heading.

The structure for ECDSA signatures shall be as per RFC 5480.

`extensions`

Organisation Certificates shall contain the `extensions` described below. They SHOULD NOT contain any additional `extensions`:

- `certificatePolicy`
- `keyUsage`
- `authorityKeyIdentifier`
- `subjectKeyIdentifier`

Cryptographic Primitives for Signature Method

Signature Method (ECDSA)

The ECDSA signature method is defined in NIST FIPS 186-4. When implementing ECDSA, the SHA-256 message digest algorithm and the P-256 elliptic curve as defined in FIPS 186-4 Annex D, D.1.2.3, shall be used.

The signature algorithm shall be `ecdsa-with-SHA256` as specified in RFC 5759. The algorithm identifier is:

```
ecdsa-with-SHA256 OBJECT IDENTIFIER ::= { iso(1) member-
body(2) us(840) ansi-X9-62(10045) signatures(4) ecdsa-with-
sha2(3) 2 }
```

SHA-256 hash algorithm

The hash algorithm used shall be the SHA-256 secure hash algorithm as defined in NIST FIPS 180-4.

Root OCA Certificate Profile

Field Name	RFC 5759/5280 Type	Value	Reference
`version`	`INTEGER`	v3	
`serialNumber`	`INTEGER`	Positive Integer of up to 16 Octets	
`signature`	`AlgorithmIdentifier`	SHA256 with ECDSA	
The value field of the `AttributeTypeAndValue` structure within the `subject` field whose type is `id-at-`	`UTF8String`	Globally unique common name of Root OCA of up to 4 Octets	

commonName (the “Issuer X520 Common Name”)			
keyIdentifier in SubjectKeyIdentifier (the "Subject Key Identifier")	keyIdentifier	A unique value that matches the subjectKeyIdentifier of the issuer’s credential	
notBefore	Time	Creation time of the Certificate	
notAfter	Time	Expiry time of the Certificate	
The value field of the AttributeTypeAndValue structure within the subject field whose type is id-at-commonName (the “Subject X520 Common Name”)	UTF8String	Globally unique name of Root OCA of up to 4 Octets (same as Issuer name)	
The value field of the AttributeTypeAndValue structure within the subject field whose type is id-at-organizationalUnitName (the “Subject X520 Organizational Unit Name”)	UTF8String	Remote Party Role of the subject of the Certificate	

`subjectPublicKeyInfo`	`SubjectPublicKeyInfo`	The Subject’s Public Key	
The `extnValue` in the `extension` whose `extnID` is `id-pe-WrappedApexContingencyKey`	`ApexContingencyKey`	The Subject’s protected (encrypted) Public Key used for recovery purposes	
`extensions`	`Extensions`	Critical and non-critical extensions	
`signatureAlgorithm`	`AlgorithmIdentifier`	SHA256 with ECDSA	
`signatureValue`	`BIT STRING`	Subject Certificate signature	

These certificates are the root of trust for the Organisations SMKI.

`version`

The version of the X.509 Certificate. Valid Certificates shall identify themselves as version 3.

`serialNumber`

Certificate serial number, a positive integer of up to 16 octets. The `serialNumber` identifies the Certificate, and shall be created by the OCA that signs the Certificate (self-signed by Root OCA). The `serialNumber` shall be unique in the scope of Certificates signed by the OCA.

`signature`

The identity of the signature algorithm used to sign the Certificate. The field is identical to the value of the Root OCA Certificate’s signatureAlgorithm field explained further under the next `signatureAlgorithm` heading.

Issuer X520 Common Name

The name of the signer of the Certificate. This will be the gloablly unique name of the Root OCA of up to 4 Octets. This will be the same as the `subject` as it is self-signed by the Root OCA.

Subject Key Identifier

The `SubjectKeyIdentifier` extension shall be included and marked as non-critical in the Certificate.

`validity`

The time period over which the issuer expects the Certificate to be valid. The validity period is the period of time from `notBefore` through `notAfter`, inclusive.

All times shall be stated in the Universal Coordinated Time (UTC) time zone. Times up to and including 23:59:59 December 31, 2049 UTC shall be encoded as `UTCTime` as YYMMDDHHmmssZ.

Times later than 23:59:59 December 31, 2049 UTC shall be encoded as `GeneralizedTime` as YYYYMMDDHHmmssZ.

`notBefore`

The earliest time a Certificate may be used. This shall be the time the Certificate is created.

`notAfter`

The latest time a Certificate is expected to be used. The value in a `notAfter` field shall be treated as specified in RFC 5280.

Subject X520 Common Name

This field must be populated with the globally unique name of the Root OCA of up to 4 Octets.

Subject X520 Organizational Unit Name

The Subject X520 `OrganizationalUnitName` attribute of `subject` shall be populated with the Remote Party Role Code that the Certificate allows the subject of the Certificate to perform.

subjectPublicKeyInfo

The Certificate's `subjectPublicKeyInfo` field shall indicate the Public Key algorithm identifier and the Public Key in the specified algorithm format as specified in RFC 3279 and RFC 5480.

The algorithm field in the `subjectPublicKeyInfo` structure shall be use the following identifier:

```
id-ecPublicKey OBJECT IDENTIFIER ::= {iso(1) member-body(2)
us(840) ansi-X9-62(10045) keyType(2) 1 }
```

`id-ecPublicKey` indicates that the algorithms that can be used with the subject Public Key are unrestricted. The key is only restricted by the values indicated in the `KeyUsage` Certificate extension (explained further under the next **`extensions`** heading).

The parameter for `id-ecPublicKey` is as follows and shall always be present:

```
ECParameters ::= CHOICE {

    namedCurve         OBJECT IDENTIFIER

    -- implicitCurve   NULL

    -- specifiedCurve  SpecifiedECDomain

  }
```

Only the following field in ECParameters shall be used:

o namedCurve - identifies all the required values for a particular set of elliptic curve domain parameters to be represented by an `OBJECT IDENTIFIER`.

The object identifier fo the curve choice to be used in OCA Certificates is:

```
secp256r1 OBJECT IDENTIFIER ::= { iso(1) member-body(2)
us(840) ansi-X9-62(10045) curves(3) prime(1) 7 }
```

The `subjectPublicKey` from `SubjectPublicKeyInfo` is the ECC Public Key.

Implementations of Elliptic Curve Cryptography according to this document shall only support the uncompressed form.

The first octet of the `subjectPublicKey` indicates whether the key is compressed or uncompressed. The uncompressed form is indicated by 0x04 (the compressed form is indicated by either 0x02 or 0x03). The Public Key shall be rejected if any value other than 0x04 is in the first octet.

`signatureAlgorithm`

The `signatureAlgorithm` field shall indicate the Root OCA signature algorithm used to sign this Certificate as defined in section under the next **Signature Method (ECDSA)** heading.

`signatureValue`

The Root OCA's signature of the Certificate shall be computed using the Root OCA's private signing key using the algorithm identified under the next **Signature Method (ECDSA)** heading.

The structure for ECDSA signatures shall be as per RFC 5480.

`extensions`

Certificates shall contain the `extensions` described below. They SHOULD NOT contain any additional `extensions`:

- `certificatePolicy`
- `keyUsage`
- `basicConstraints`
- `subjectKeyIdentifer`

Cryptographic Primitives for Signature Method

Signature Method (ECDSA)

The ECDSA signature method is defined in NIST FIPS 186-4. When implementing ECDSA, the SHA-256 message digest algorithm and the P-256 elliptic curve as defined in FIPS 186-4 Annex D, D.1.2.3, shall be used.

The signature algorithm shall be `ecdsa-with-SHA256` as specified in RFC 5759. The algorithm identifier is:

```
ecdsa-with-SHA256 OBJECT IDENTIFIER ::= { iso(1) member-
body(2) us(840) ansi-X9-62(10045) signatures(4) ecdsa-with-
sha2(3) 2 }
```

SHA-256 hash algorithm

The hash algorithm shall be the SHA-256 secure hash algorithm as defined in NIST FIPS 180-4.

Issuing OCA Certificate Profile

Field Name	RFC 5759/5280 Type	Value	Reference
`version`	`INTEGER`	v3	
`serialNumber`	`INTEGER`	Positive Integer of up to 16 Octets	
`signature`	`AlgorithmIdentifier`	SHA256 with ECDSA	
The `value` field of the `AttributeTypeAndValue` structure within the `subject` field whose `type` is `id-at-`	`UTF8String`	Globally unique name of Root OCA of up to 4 Octets (as defined in the	

commonName (the "Issuer X520 Common Name")		Root OCA Certificate Profile)	
keyIdentifier in subjectKeyIdentifier (the "Subject Key Identifier")	keyIdentifier	Provides a means for identifying certificates containing the particular Public Key used in an application	
keyIdentifier in authorityKeyIdentifier (the "Authority Key Identifier")	keyIdentifier	A unique value that matches the subjectKeyIdentifier value of the issuer's credential	
notBefore	Time	Creation time of the certificate	
notAfter	Time	Expiry time of the Certificate	
The value field of the AttributeTypeAndValue structure within the subject field whose type is id-at-commonName (the "Subject X520 Common Name")	UTF8String	Globally unique name of Issuing OCA of up to 4 Octets	
The value field of the AttributeTypeAndValue structure within the subject field	UTF8String	Remote Party Role of the Subject of the Certificate	

whose `type` is `id-at-organizationalUnitName` (the "Subject X520 Organizational Unit Name")			
`subjectPublicKeyInfo`	`SubjectPublicKeyInfo`	The Subject's Public Key	
`extensions`	`Extensions`	Critical and non-critical extensions	
`signatureAlgorithm`	`AlgorithmIdentifier`	SHA256 with ECDSA	
`signatureValue`	`BIT STRING`	Subject certificate signature	

`version`

The version of the X.509 Certificate. Valid Certificates shall identify themselves as version 3.

`serialNumber`

Certificate serial number, a positive integer of up to 16 octets. The serialNumber identifies the Certificate, and shall be created by the Root OCA that signs the Certificate. The serialNumber shall be unique in the scope of Certificates signed by the Root OCA.

`signature`

The identity of the signature algorithm used to sign the Certificate. The field is identical to the value of the Issuing OCA Certificate's `signatureAlgorithm` field explained further under the next **`signatureAlgorithm`** heading.

Issuer X520 Common Name

The name of the signer of the Certificate. This will be the gloablly unique name of the Root OCA of up to 4 Octets (as defined in the Root OCA Certificate Profile).

Subject Key Identifier

The `SubjectKeyIdentifier` extension shall be included and marked as non-critical in the Certificate.

Authority Key Identifier

To optimize building the correct credential chain, the non-critical `AuthorityKeyIdentifier` extension shall be populated with a unique value as recommended by RFC 5280 and shall be included in all Organisation Certificates.

`validity`

The time period over which the issuer expects the Certificate to be valid. The `validity` period is the period of time from `notBefore` through `notAfter`, inclusive.

All times shall be stated in the Universal Coordinated Time (UTC) time zone. Times up to and including 23:59:59 December 31, 2049 UTC shall be encoded as `UTCTime` as YYMMDDHHmmssZ.

Times later than 23:59:59 December 31, 2049 UTC shall be encoded as `GeneralizedTime` as YYYYMMDDHHmmssZ.

`notBefore`

The earliest time a Certificate may be used. This shall be the time the Certificate is created.

`notAfter`

The latest time a Certificate is expected to be used. The value in a `notAfter` field shall be treated as specified in RFC 5280.

Subject X520 Common Name

This field shall be populated with the globally unique name of the Issuing OCA of up to 4 Octets.

Subject X520 Organizational Unit Name

The Subject X520 Organizational Unit Name attribute of subject shall be populated with the Remote Party Role Code that the Certificate allows the subject of the Certificate to perform.

`subjectPublicKeyInfo`

The Certificate's `subjectPublicKeyInfo` field shall indicate the Public Key algorithm identifier and the Public Key in the specified algorithm format as specified in RFC 3279 and RFC 5480.

The algorithm field in the `subjectPublicKeyInfo` structure shall contain the following identifier:

```
id-ecPublicKey OBJECT IDENTIFIER ::= {iso(1) member-body(2)
us(840) ansi-X9-62(10045) keyType(2) 1 }
```

`id-ecPublicKey` indicates that the algorithms that can be used with the subject Public Key are unrestricted. The key is only restricted by the values indicated in the `KeyUsage` Certificate extension (explained further under the next **`extensions`** heading).

The parameter for `id-ecPublicKey` is as follows and shall always be present:

```
ECParameters ::= CHOICE {

    namedCurve         OBJECT IDENTIFIER

    -- implicitCurve   NULL

    -- specifiedCurve  SpecifiedECDomain

  }
```

Only the following field in ECParameters shall be used:

o `namedCurve` - identifies all the required values for a particular set of elliptic curve domain parameters to be represented by an

OBJECT IDENTIFIER.

The object identifier fo the curve choice to be used in Certificates is:

```
secp256r1 OBJECT IDENTIFIER ::= { iso(1) member-body(2)
us(840) ansi-X9-62(10045) curves(3) prime(1) 7 }
```

The subjectPublicKey from SubjectPublicKeyInfo is the ECC Public Key.

Implementations of Elliptic Curve Cryptography according to this document shall only support the uncompressed form.

The first octet of the subjectPublicKey indicates whether the key is compressed or uncompressed. The uncompressed form is indicated by 0x04 (the compressed form is indicated by either 0x02 or 0x03). The Public Key MUST be rejected if any value other than 0x04 is included in the first octet.

signatureAlgorithm

The signatureAlgorithm field shall indicate the Root OCA signature algorithm used to sign this Certificate as defined under the next **Signature Method (ECDSA)** heading.

signatureValue

The Root OCA's signature of the Certificate shall be computed using the Root OCA's private signing key using the algorithm identified under the next **Signature Method (ECDSA)** heading.

The structure for ECDSA signatures shall be as per RFC 5480.

extensions

Issuing-CA Certificates shall contain the extensions described below. They SHOULD NOT contain any additional extensions:

- certificatePolicy
- keyUsage

- `basicConstraints`
- `subjectKeyIdentifer`
- `authorityKeyIdentifier`

Cryptographic Primitives for Signature Method

Signature Method (ECDSA)

The ECDSA signature method is defined in NIST FIPS 186-4. When implementing ECDSA, the SHA-256 message digest algorithm and the P-256 elliptic curve as defined in FIPS 186-4 Annex D, D.1.2.3, shall be used.

The signature algorithm shall be `ecdsa-with-SHA256` as specified in RFC 5759. The algorithm identifier is:

```
ecdsa-with-SHA256 OBJECT IDENTIFIER ::= { iso(1) member-
body(2) us(840) ansi-X9-

62(10045) signatures(4) ecdsa-with-sha2(3) 2 }
```

SHA-256 hash algorithm

The hash algorithm used shall be the SHA-256 secure hash algorithm as defined in NIST FIPS 180-4.

Version C 3.0

Appendix C

SMKI Compliance Policy

Contents

1 INTRODUCTION

1.1 The document comprising this Appendix C:

(a) shall be known as the "**SMKI Compliance Policy**" (and in this document is referred to simply as the " **Policy**"),

(b) is a SEC Subsidiary Document related to Section L2 of the Code (SMKI Assurance).

2 SMKI INDEPENDENT ASSURANCE SCHEME

DCC: Duty to Submit to an SMKI Independent Assurance Scheme

2.1 The DCC shall subject the SMKI Services to assessment against an assurance scheme which satisfies:

(a) the quality requirements specified in Part 2.2 of this Policy;

(b) the independence requirements specified in Part 2.3 of this Policy; and

(c) the approval requirements specified in Part 2.5 of this Policy,

and that scheme is referred to in this Policy as the "**SMKI Independent Assurance Scheme**".

Quality Requirements

2.2 The quality requirements specified in this Part 2.2 are that the SMKI Independent Assurance Scheme must be a scheme:

(a) which is recognised as an accreditation scheme for the purposes of the eIDAS Regulation (No 910/2014 of the European Parliament and of the Council of 23 July 2014 on electronic identification and trust services for electronic transactions in the internal market).

(b) which is based on ISO 27001; and

(c) the provider of which:

(i) is used by the United Kingdom Government to provide assurance in relation to electronic trust services; and

(ii) requires all its scheme assessors to be UKAS certified.

Independence Requirements

2.3 The independence requirements specified in this Part 2.3 are that the provider of the SMKI Independent Assurance Scheme must be independent of the DCC and of each DCC Service Provider from which the DCC acquires capability for the purposes of the provision of the SMKI Services (referred to in this Policy as a " **Relevant DCC Service Provider**").

2.4 For the purposes of Part 2.3 of this Policy, the provider of the SMKI Independent Assurance Scheme is to be treated as independent of the DCC (and of Relevant DCC Service Providers) only if:

(a) neither the DCC nor any of its subsidiaries (or any Relevant DCC Service Provider or any of its subsidiaries) holds or acquires any investment by way of shares, securities or other financial rights or interests in the provider of the scheme;

(b) either:

(i) no director or employee of the DCC (or of any Relevant DCC Service Provider) is or becomes a director or employee of the provider of the scheme; or

(ii) where any person is or becomes both a director or employee of the DCC (or of any Relevant DCC Service Provider) and a director or employee of the provider of the scheme, appropriate arrangements are in place to ensure that that person is able to have no influence on any decisions made by the provider of the scheme in respect of the approval of any person or the accreditation of any thing in accordance with the scheme;

(c) no person who is a director or employee of the DCC (or of any Relevant DCC Service Provider) holds or acquires any investment by way of shares, securities or other financial rights or interests in the provider of the scheme, except where sub-paragraph (b)(ii) applies and that investment is acquired by that person by way of reasonable compensation for his or her performance as a director or employee of the provider of the scheme; and

(d) the provider of the scheme does not hold or acquire a participating interest (as defined in section 421A of the Financial Services and Markets Act 2000) in the DCC (or in any Relevant DCC Service Provider).

Approval Requirements

2.5 Before entering into any agreement with the provider of the SMKI Independent Assurance Scheme, in accordance with its obligation under Section L2.2 of the Code (SMKI Compliance Policy), the DCC shall submit to the SMKI PMA for approval:

(a) its proposed choice of scheme; and

(b) the proposed terms and conditions of its agreement with the provider of that scheme,

and shall not enter into any such agreement unless the SMKI PMA has first approved the proposed SMKI Independent Assurance Scheme and the proposed terms and conditions of that agreement.

2.6 If the SMKI PMA does not approve either the proposed SMKI Independent Assurance Scheme or the proposed terms and conditions of the DCC's agreement with the provider of that scheme:

(a) the SMKI PMA shall provide the DCC with a statement of its reasons for not doing so; and

(b) the DCC shall submit to the SMKI PMA for approval, as soon as is reasonably practicable, a revised proposal in relation to the scheme.

3 INDEPENDENT ASSURANCE SERVICE PROVIDER

DCC: Duty to Procure Independent Assurance Services

3.1 For the purposes of complying with its obligation under Section L2.2 of the Code (SMKI Compliance Policy), the DCC shall procure the provision of assurance services:

(a) of the scope specified in Part 3.2 of this Policy;

(b) from a person who:

(i) is suitably qualified in accordance with Part 3.3 of this Policy; and

(ii) satisfies the independence requirements specified in Part 3.4 of this Policy,

and that person is referred to in this Policy as the "**Independent SMKI Assurance Service Provider**".

Scope of Independent Assurance Services

3.2 The assurance services specified in this Part 3.2 are services in accordance with which the Independent SMKI Assurance Service Provider shall:

(a) undertake an initial assessment of the SMKI Services against the SMKI Independent Assurance Scheme in accordance with Part 4 of this Policy;

(b) subsequently undertake further assessments of the SMKI Services against the SMKI Independent Assurance Scheme:

(i) at a frequency recommended by the provider of that scheme; or

(ii) where there is no such recommended frequency, or where the SMKI PMA otherwise determines, at a frequency specified by the SMKI PMA;

(c) at the request of, and to an extent determined by, the SMKI PMA, carry out an assessment of the compliance of any SMKI Participant with the applicable requirements of the SMKI Document Set;

(d) at the request of the SMKI PMA, provide to it advice in relation to the compliance of any SMKI Participant with the applicable requirements of the SMKI Document Set;

(e) at the request of the SMKI PMA, provide to it advice in relation to a review of this Policy, which shall include in particular:

(i) recommendations as to the scope and frequency of assessments carried out in accordance with this Policy; and

(ii) advice in relation to the suitability of any remedial action plan for the purposes of Section M8.4 of the Code (Consequences of an Event of Default), including where the Defaulting Party is the DCC in accordance with Section L2.6 of the Code (Events of Default); and

(f) at the request of the SMKI PMA Chair, provide a representative to attend and contribute to the discussion at any meeting of the SMKI PMA.

Suitably Qualified Service Provider

3.3 The Independent SMKI Assurance Service Provider shall be treated as suitably qualified in accordance with this Part 3.3 only if it is recognised by the provider of the SMKI Independent Assurance Scheme as being qualified to carry out assessments against that scheme.

Independence Requirements

3.4 The independence requirements specified in this Part 3.4 are that the Independent SMKI Assurance Service Provider must be independent of each SMKI Participant and of each service provider from whom that SMKI Participant acquires capability for any purpose related to its compliance with its obligations under the Code (but excluding any provider of corporate assurance services to that SMKI Participant).

3.5 For the purposes of Part 3.4 of this Policy, the Independent SMKI Assurance Service Provider is to be treated as independent of an SMKI Participant (and of a relevant service provider of that SMKI Participant) only if:

(a) neither that SMKI Participant nor any of its subsidiaries (or such a service provider or any of its subsidiaries) holds or acquires any investment by way of shares, securities or other financial rights or interests in the Independent SMKI Assurance Service Provider;

(b) no director of that SMKI Participant (or of any such service provider) is or becomes a director or employee of, or holds or acquires any investment by way of shares, securities or other financial rights or interests in, the Independent SMKI Assurance Service Provider; and

(c) the Independent SMKI Assurance Service Provider does not hold or acquire a participating interest (as defined in section 421A of the Financial Services and Markets Act 2000) in that SMKI Participant (or in any such service provider).

4 INITIAL ASSURANCE ASSESSMENT

DCC: Duty to Procure Initial Assessment

4.1 The DCC shall ensure that an initial assurance assessment of the SMKI Services:

(a) against the SMKI Independent Assurance Scheme; and

(b) in respect of compliance by the DCC with the applicable requirements of the SMKI Document Set,

is undertaken by the Independent SMKI Assurance Service Provider in accordance with Part 4.2 of this Policy.

Nature of the Initial Assessment

4.2 The initial assessment referred to in Part 4.1 of this Policy shall be undertaken in two stages, as described in Parts 4.3 and 4.5 of this Policy.

4.3 The first stage of the initial assessment shall:

(a) be undertaken by no later than such date as is necessary in order to ensure that an assessment report may be produced in accordance with paragraph (b); and

(b) result in an assessment report to be known as the "**Stage 1 Assurance Report**" in relation to the SMKI Services being produced by the Independent SMKI Assurance Service Provider by no later than such date as the SMKI PMA shall determine.

4.4 The Stage 1 Assurance Report shall:

(a) clearly identify any failure of the DCC to comply with the applicable requirements of the SMKI Document Set;

(b) recommend that the assurance status of the DCC in relation to the SMKI Services should be set at:

(i) approved;

(ii) approved with caveats; or

(iii) not approved; and

(c) be provided to both the DCC and the SMKI PMA promptly upon completion.

4.5 The second stage of the initial assessment shall:

(a) be undertaken by no later than such date as is necessary in order to ensure that an assessment report may be produced in accordance with paragraph (b); and

(b) result in an assessment report to be known as the "**Stage 2 Assurance Report**" in relation to the SMKI Services being produced by the Independent SMKI Assurance Service Provider by no later than such date as the SMKI PMA shall determine.

4.6 The Stage 2 Assurance Report shall:

(a) clearly identify any failure of the DCC to comply with the applicable requirements of the SMKI Document Set;

(b) recommend that the assurance status of the DCC in relation to the SMKI Services should be set at:

(i) approved;

(ii) approved with caveats; or

(iii) not approved; and

(c) be provided to both the DCC and the SMKI PMA promptly upon completion.

PMA: Response to the Initial Assessment

4.7 On receiving either the Stage 1 Assurance Report or Stage 2 Assurance Report, the SMKI PMA shall:

(a) promptly consider that report;

(b) determine that the assurance status of the DCC in relation to the SMKI Services is to be set at:

(i) approved;

(ii) approved with caveats; or

(iii) not approved;

(c) where the SMKI PMA has set the assurance status of the DCC in relation to the SMKI Services at ‘approved with caveats’, state in writing its reasons for considering that it is acceptable for the DCC to:

(i) in the case of the Stage 1 Assurance Report, commence the provision of the SMKI Services; or

(ii) in the case of the Stage 2 Assurance Report, continue to provide the SMKI Services; and

(d) provide a copy of the report (being redacted only in so far as necessary for the purposes of security) and a statement of its determination (and of any reasons accompanying that determination) to all Parties.

4.8 Where the SMKI PMA has set the assurance status of the DCC in relation to the SMKI Services at ‘approved with caveats’ or ‘not approved’ it shall:

(a) require that the DCC submit to it as soon as reasonably practicable a remedial action plan; and

(b) within one month of the submission of that plan, require the DCC to make any changes to it that the SMKI PMA may specify.

DCC: Duty in relation to Remedial Action Plan

4.9 Where the DCC is required to do so in accordance with Part 4.8(a) of this Policy, it shall as soon as reasonably practicable submit to the SMKI PMA a remedial action plan.

4.10 Where the DCC is required by the SMKI PMA in accordance with Part 4.8(b) of this Policy to make changes to the remedial action plan, it may appeal that decision to the Authority and:

(a) the Authority shall determine what changes (if any) shall be made to the remedial action plan; and

(b) the determination of the Authority shall be final and binding for the purposes of the Code.

4.11 The DCC shall implement any remedial action plan subject to any required changes to it specified by:

(a) the SMKI PMA in accordance with Part 4.8(b) of this Policy; or

(b) the Authority in accordance with Part 4.10 of this Policy.

5 PMA: DUTY TO PROVIDE INFORMATION

Initial Assurance Assessment

5.1 The SMKI PMA shall, on request, provide to the Secretary of State and the Authority a copy of:

(a) the Stage 1 Assurance Report received by it in accordance with Part 4.4 of this Policy;

(b) the Stage 2 Assurance Report received by it in accordance with Part 4.6 of this Policy; and

(c) any remedial action plan that the DCC is required to implement in accordance with Part 4.11 of this Policy.

Subsequent Assurance Assessments

5.2 Following any assessment carried out by the Independent SMKI Assurance Service Provider of the compliance of the DCC with the applicable requirements of the SMKI Document Set, the SMKI PMA's determination as to the extent to which the DCC is compliant with those requirements shall be made available by it to:

(a) all Parties;

(b) the Panel;

(c) the Authority; and

(d) on request, the Secretary of State.

5.3 On receiving any subsequent assurance report, the SMKI PMA shall:

(a) promptly consider that report;

(b) determine that the assurance status of the DCC in relation to the SMKI Services is to be set at:

(i) approved;

(ii) approved with caveats; or

(iii) not approved;

(c) where the SMKI PMA has set the assurance status of the DCC in relation to the SMKI Services at ‘approved with caveats’, state in writing its reasons for considering that it is acceptable for the DCC to commence the provision of the SMKI Services; and

(d) provide a summary of any non-compliances and a SMKI PMA statement of its determination (and of any reasons accompanying that determination) to all Parties.

5.4 Where the SMKI PMA has set the assurance status of the DCC in relation to the SMKI Services at ‘approved with caveats’ or ‘not approved’ it shall:

(a) require that the DCC submit to it as soon as reasonably practicable a remedial action plan; and

(b) within one month of the submission of that plan, require the DCC to make any changes to it that the SMKI PMA may specify.

5.5 Where the DCC is required by the SMKI PMA in accordance with Part 5.4 of this Policy to make changes to the remedial action plan, it may appeal that decision to the SEC Panel and:

(a) the SEC Panel shall determine what changes (if any) shall be made to the remedial action plan; and

(b) the determination of the SEC Panel shall be final and binding for the purposes of the Code.

5.6 The DCC shall implement any remedial action plan subject to any required changes to it specified by:

(a) the SMKI PMA in accordance with Part 5.4 of this Policy; or

(b) the SEC Panel in accordance with Part 5.5 of this Policy.

APPENDIX D

SMKI Registration Authority Policies and Procedures

(SMKI RAPP)

Contents

1. Introduction

1.1 Purpose

Section L9.6 of the Code sets out the process for the DCC to develop the SMKI Registration Authority Policies and Procedures (SMKI RAPP) as a SMKI SEC Document as defined in Section L 9.4 (a) (v).

The SMKI RAPP sets out the principal obligations and activities undertaken by the DCC in its capacity as the SMKI Registration Authority in accordance with Section L of the Code, and Appendices A, B and Q of the Code. The SMKI RAPP also sets out the activities undertaken by the SMKI Registration Authority in support of the procedures set out in the DCCKI RAPP, as set out in Section 2 of this document.

2. SMKI Registration Authority obligations to support DCCKI identity verification

The DCCKI RAPP sets out the procedures by which nominated individuals may become DCCKI Senior Responsible Officers and/or DCCKI Authorised Responsible Officers in order to act on behalf of a Party, RDP or a DCC Service Provider in respect of DCCKI Services and the DCCKI Repository Service. The DCCKI RAPP also sets out the activities undertaken by the DCC as DCCKI Registration Authority.

Upon request from the DCCKI Registration Authority to verify the identity of an individual nominated to be a DCCKI SRO or DCCKI ARO, the SMKI Registration Authority shall:

a) arrange a verification meeting with the nominated individual, at a date and time that is mutually agreed;

b) at the verification meeting, verify the individual identity of the nominated individual to the level pursuant to the SMKI PMA Guidance on "Verifying Individual Identity" published on the Website, or except to the extent that the DCC otherwise notifies the SMKI Registration Authority, to such equivalent level within a comparable authentication framework as may be agreed by the SMKI PMA for the purposes of verification of individuals to become a SMKI SRO or SMKI ARO;

c) following the verification meeting, notify the nominated individual whether the process to verify their individual identity has been successful; and

d) following the verification meeting, notify the DCCKI Registration Authority whether the identity of the individual has been successfully verified.

Provided that the DCC need not repeat these processes in relation to an individual for the purposes of verifying their identity for the purposes of becoming a DCCKI SRO and/or DCCKI ARO where the required verification processes have already been carried out for the purposes of identifying them as being an SMKI SRO and/or SMKI ARO respectively.

The DCC and any Party or RDP may agree that any action taken by either of them prior to the date of the designation of this SMKI RAPP shall, if the equivalent action taken after that date would have satisfied a requirement of this SMKI RAPP for the purposes of appointing a DCCKI ARO or DCCKI SRO, be treated as if it had taken place after that date.

3. SMKI Roles

This SMKI RAPP details the roles of Parties, RDPs, Manufacturers, SECCo and the DCC in the context of access to SMKI Services and/or the SMKI Repository Service as set out in the Code, this SMKI RAPP and the SMKI interface documents. The SMKI RAPP sets out the procedures by which nominated individuals may become Senior Responsible Officers and/or Authorised Responsible Officers in order to act on behalf of a Party, RDP, Manufacturer, SECCo or the DCC (acting in its role as DCC Service Provider) in respect of SMKI Services and the SMKI Repository Service.

This SMKI RAPP also details the obligations in respect of the SMKI Registration Authority and the individuals acting on its behalf as SMKI Registration Authority Managers or SMKI Registration Authority Personnel.

From time to time, the SMKI PMA may require documents or information to be lodged in the SMKI Repository. In such instances, it shall submit a request via the Service Desk and provide such documents and/or information to be lodged in the SMKI Repository. The DCC shall lodge documents and/or information provided to the SMKI Repository, as soon as reasonably practicable following receipt.

3.1 Party, RDP, Manufacturer, SECCo and DCC representatives

Individuals permitted to act as representatives of a Party, RDP, Manufacturer, SECCo or the DCC (in its role as DCC Service Provider) are as set out immediately below:

- **Senior Responsible Officer (SRO)**. The process by which an individual is nominated and their authorisation is checked and their identity verified, so as to be an SRO and act on behalf of an organisation is set out in SMKI RAPP Section 5.2. An individual is nominated to become an SRO by a Director or Company Secretary for a Party, RDP, Manufacturer, SECCo or the DCC (for DCC Service Provider personnel). Once an individual has become an SRO, the SRO may at any time nominate individuals to undertake to become Authorised Responsible Officers (AROs) and to access SMKI Services and/or the SMKI Repository Service. An SRO may also nominate themselves to become an ARO as described below.

- **Authorised Responsible Officer (ARO)**. The process by which an individual is nominated, verified and authorised to be an ARO is set out in SMKI RAPP Section 5.3. The means by which AROs are provided with credentials to authenticate access to SMKI Services and/or the SMKI Repository Service is set out in Section 5.4. The DCC shall permit only AROs to act on behalf of a Party, RDP, Manufacturer, SECCo or the DCC (in its role as DCC Service Provider) for the purposes of accessing SMKI Services and/or the SMKI Repository Service. Depending upon the processes followed, an ARO may also be authorised to act on behalf of a Party, RDP or the DCC (in its role as DCC Service Provider) to be an Authorised Subscriber for Organisation Certificates, Device Certificates or both, following successful completion of SMKI and Repository Entry Process Tests. All AROs are also permitted to access the SMKI Repository Service on behalf of the organisation that they represent, as set out in the SMKI Repository Interface Design Specification.

Each Party, RDP, Manufacturer, SECCo or the DCC (in its role as DCC Service Provider) that wishes to:

a) become an Authorised Subscriber for Organisation Certificates and/or Device Certificates;

b) become an Authorised Subscriber for an IKI Certificate for the purposes of Digitally Signing of files; or

c) have access only to the SMKI Repository,

shall have at least one ARO successfully appointed (and therefore one SRO).

The DCC shall not be required to repeat processes in relation to an individual for the purposes of verifying their identity for the purposes of becoming an SRO and/or ARO in respect of SMKI Services or the SMKI Repository Service, where the required verification processes have already been carried out for the purposes of identifying them as being a DCCKI SRO and/or DCCKI ARO respectively.

The DCC and any Party or RDP may agree that any action taken by either of them prior to the date of the designation of this SMKI RAPP shall, if the equivalent action taken after that date would have satisfied a requirement of this SMKI RAPP for the purposes of appointing an ARO or SRO or the Party or RDP becoming an Authorised Subscriber, be treated as if it had taken place after that date.

3.2 SMKI Registration Authority representatives

Individuals acting as representatives of the DCC in its role as SMKI Registration Authority are:

- **SMKI Registration Authority Manager**. The process by which a SMKI Registration Authority Manager is nominated, verified, authorised and provided with the means to authenticate their access to SMKI Services and/or the SMKI Repository Service is set out in SMKI RAPP Sections 6.2 and 6.4.

- **SMKI Registration Authority Personnel.** The process by which SMKI Registration Authority Personnel are nominated, verified, authorised and provided with the means to authenticate their access to SMKI Services and/or SMKI Repository is set out in SMKI RAPP Sections 6.3 and 6.4.

The DCC shall ensure that only a SMKI Registration Authority Manager or SMKI Registration Authority Personnel may act on behalf of the DCC in respect of matters relating to the SMKI Registration Authority. Each Party, RDP, Manufacturer, SECCo and the DCC (in its role of DCC Service Provider) shall refrain from dealing with DCC Personnel (including SMKI Registration Authority Managers and SMKI Registration Authority Personnel) other than as directed by the Service Desk for the purposes of submitting Certificate Signing Requests (CSRs) and Certificate Revocation Requests (CRRs).

The DCC, in order to perform its role as SMKI Registration Authority, shall nominate at least two individuals to become a SMKI Registration Authority Manager, each of which will have responsibility for:

a) management of the SMKI Registration Authority function and SMKI Registration Authority Personnel;

b) nomination of individuals to become SMKI Registration Authority Personnel;

c) authentication and verification of SMKI Registration Authority Personnel, as set out in Section 6.3 of this document;

d) provision of the means to authenticate access to SMKI Services and/or the SMKI Repository Service for authorised Party, RDP, Manufacturer or SECCo representatives and DCC Personnel (including SMKI Registration Authority Personnel);

e) managing the process by which documents and information are lodged in the SMKI Repository; and

f) approval of CRRs.

A SMKI Registration Authority Manager may nominate individuals to become SMKI Registration Authority Personnel and to act on behalf of the SMKI Registration Authority as set out in this SMKI RAPP and the Code. The primary responsibilities of SMKI Registration Authority Personnel are:

a) to conduct registration processes as set out in SMKI RAPP Sections 5.1 to 5.5, incorporating:

   i. verification of organisational identity;

   ii. verification and authorisation of individuals nominated to become SROs or AROs, as set out in Section 5.2 and 5.3 of this document;

   iii. provision of the means to authenticate access to SMKI Services and/or the SMKI Repository Service for authorised Party, RDP, Manufacturer, SECCo representatives and DCC personnel; and

   iv. assessment of whether an organisation qualifies to become an Authorised Subscriber for Organisation Certificates and/or Device Certificates.

b) processing and approval (where required) of Certification Signing Requests and processing of Certificate Revocation Requests; and

c) processing of requests for revocation of credentials used to access SMKI Services and/or the SMKI Repository Service.

The DCC shall ensure that SMKI Registration Authority Managers and SMKI Registration Authority Personnel, where required, are available to undertake the obligations in respect of procedures set out in this SMKI RAPP:

a) in respect of the verification, processing and approval of CRRs, on a 24*7 basis; and

b) in respect of all other procedures as set out in this SMKI RAPP, on a Working Day basis and during standard working hours in England.

The DCC and any Party, RDP, Manufacturer or SECCo may agree that any action taken by either of them prior to the date of the designation of this SMKI RAPP shall, if the equivalent action taken after that date would have satisfied a requirement of this SMKI RAPP for the purposes of appointing a SMKI Registration Authority Manager or member of SMKI Registration Authority Personnel, be treated as if it had taken place after that date.

4. Party, RDP, Manufacturer, SECCo and DCC (as DCC Service Provider) registration procedures

4.1 General registration obligations

4.1.1 Organisation, individual, and RA obligations

Each Party, RDP, Manufacturer, SECCo and the DCC (in its role as DCC Service Provider) shall ensure that its nominated representatives wishing to access SMKI Services and/or the SMKI Repository Service shall undertake the procedures and processes as set out in SMKI RAPP Sections 5.1 to 5.5, as appropriate.

To facilitate this, the SMKI Registration Authority shall:

a) make the forms as set out in SMKI RAPP Annex A, available from the DCC Website or via the DCC SharePoint site as advised by the DCC;

b) provide reasonable support and advice to each Party, RDP, Manufacturer, SECCo and DCC Service Providers in relation to the procedures as set out in SMKI RAPP sections 5.1 to 5.5;

c) place no restriction on the number of individuals that can be nominated as SROs or AROs in respect of any Party, RDP, Manufacturer, SECCo or the DCC (in its role as DCC Service Provider);

d) permit an individual to become an ARO to represent multiple parties, by successfully completing the procedures in SMKI RAPP section 5.3 and 5.4 as are necessary;

e) store and maintain records relating to the nomination, verification and authorisation of individuals and organisations (but not the personal details of individuals) as set out Sections 5.1 to 5.5, and in accordance with the Code and the DCC's data retention policy and data protection policy;

f) not permit any nominated individual to access the SMKI Services or relevant the SMKI Repository Service on behalf of a Party, RDP, Manufacturer, SECCo or the DCC (in its role as DCC Service Provider) until they have become an ARO;

g) ensure that credentials issued under the IKI Certificate Policy to AROs have a lifetime of ten years and that such credentials and shall cease to be valid after ten years following issuance;

h) for authentication and file signing credentials issued under the IKI Certificate Policy and where the Key Pair and Certificate Signing Request are both generated by the prospective ARO on a Cryptographic Credential Token during the ARO verification meeting, that the prospective ARO has an opportunity to validate and agree information (e.g. role and other organisation and individual identity) against which the Certificate is Issued is accurate and that it reflects the identity of the ARO or system that is the subject of the Certificate;

i) for authentication and file signing credentials issued under the IKI Certificate Policy and which are delivered to the SMKI Registration Authority in the form of a Certificate Signing Request generated by the prospective ARO's organisation and provided by the prospective ARO during the ARO verification meeting, that the prospective ARO has an opportunity to validate the information in the resulting Certificate reflects that provided in the Certificate Signing Request and that it is accurate and reflects the identity of the prospective ARO or system that is the subject of the Certificate;

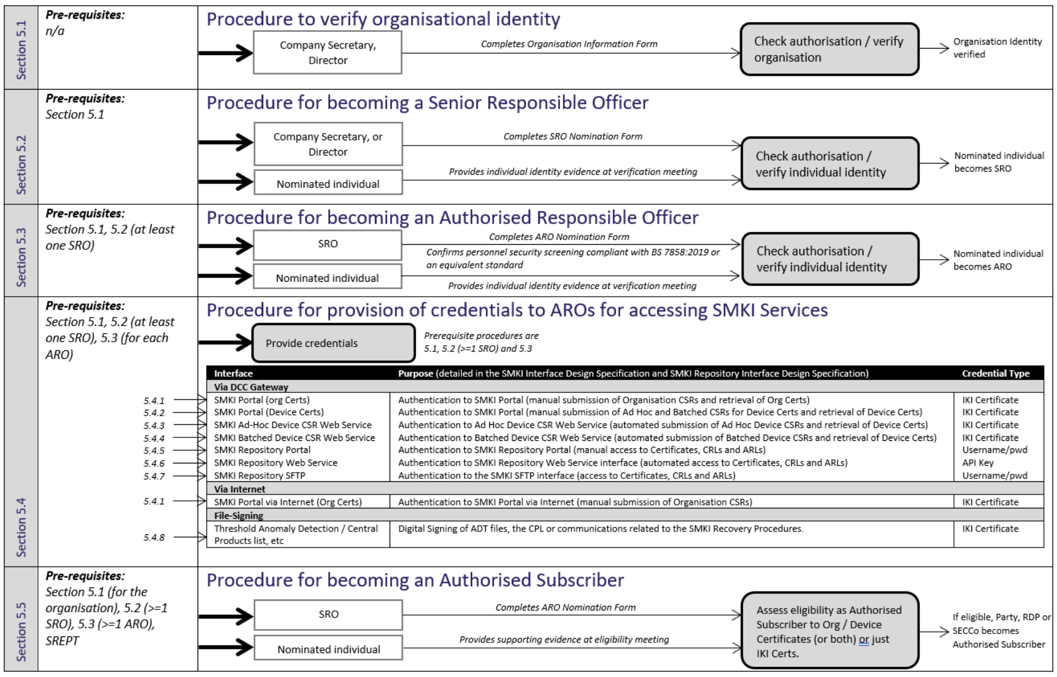
j) for authentication credentials not issued under the IKI Certificate Policy, shall ensure that such authentication credentials remain valid until revoked; and

k) produce, each month, and make available to each Party, RDP, Manufacturer and SECCo, a report for that organisation which details the list of SROs, AROs, the credentials that have been issued to each ARO and those AROs for which credentials will expire in the following month.

4.1.2 High level overview of SMKI Registration Authority procedures

Figure 1 as set out immediately below provides a high level view of the procedures required in order for a Party, RDP, Manufacturer, SECCo or the DCC (in its role as DCC Service Provider) to:

- verify their organisational identity;
- become an SRO;
- become an ARO;
- gain credentials for accessing SMKI Services and/or the SMKI Repository Service;
- become an Authorised Subscriber for:
  - Organisation Certificates or Device Certificates, or both;
  - a File Signing Certificate (issued under the IKI Certificate Policy) for the purposes of verifying Digital Signatures of files in accordance with the Code;
- gain access to Organisation Certificates and/or Device Certificates and other material via the SMKI Repository; and
- gain access to File Signing Certificates, and their corresponding Private Keys to be used for the purposes of Digitally Signing files.


Section 5.1
Pre-requisites:
n/a
Procedure to verify organisational identity
Company Secretary, Director
Completes Organisation Information Form
Check authorisation / verify organisation
Organisation Identity verified
Section 5.2
Pre-requisites:
Section 5.1
Procedure for becoming a Senior Responsible Officer
Company Secretary, or Director
Completes SRO Nomination Form
Nominated individual
Provides individual identity evidence at verification meeting
Check authorisation / verify individual identity
Nominated individual becomes SRO
Section 5.3
Pre-requisites:
Section 5.1, 5.2 (at least one SRO)
Procedure for becoming an Authorised Responsible Officer
SRO
Completes ARO Nomination Form
Confirms personnel security screening compliant with BS 7858:2019 or an equivalent standard
Nominated individual
Provides individual identity evidence at verification meeting
Check authorisation / verify individual identity
Nominated individual becomes ARO
Section 5.4
Pre-requisites:
Section 5.1, 5.2 (at least one SRO), 5.3 (for each ARO)
Procedure for provision of credentials to AROs for accessing SMKI Services
Provide credentials
Prerequisite procedures are 5.1, 5.2 (>=1 SRO) and 5.3
5.4.1
5.4.2
5.4.3
5.4.4
5.4.5
5.4.6
5.4.7
5.4.1
5.4.8
Section 5.5
Pre-requisites:
Section 5.1 (for the organisation), 5.2 (>=1 SRO), 5.3 (>=1 ARO), SREPT
Procedure for becoming an Authorised Subscriber
SRO
Completes ARO Nomination Form
Nominated individual
Provides supporting evidence at eligibility meeting
Assess eligibility as Authorised Subscriber to Org / Device Certificates (or both) or just IKI Certs.
If eligible, Party, RDP or SECCo becomes Authorised Subscriber

Interface	Purpose (detailed in the SMKI Interface Design Specification and SMKI Repository Interface Design Specification)	Credential Type
Via DCC Gateway		
SMKI Portal (org Certs)	Authentication to SMKI Portal (manual submission of Organisation CSRs and retrieval of Org Certs)	IKI Certificate
SMKI Portal (Device Certs)	Authentication to SMKI Portal (manual submission of Ad Hoc and Batched CSRs for Device Certs and retrieval of Device Certs)	IKI Certificate
SMKI Ad-Hoc Device CSR Web Service	Authentication to Ad Hoc Device CSR Web Service (automated submission of Ad Hoc Device CSRs and retrieval of Device Certs)	IKI Certificate
SMKI Batched Device CSR Web Service	Authentication to Batched Device CSR Web Service (automated submission of Batched Device CSRs and retrieval of Device Certs)	IKI Certificate
SMKI Repository Portal	Authentication to SMKI Repository Portal (manual access to Certificates, CRLs and ARLs)	Username/pwd
SMKI Repository Web Service	Authentication to SMKI Repository Web Service interface (automated access to Certificates, CRLs and ARLs)	API Key
SMKI Repository SFTP	Authentication to the SMKI SFTP interface (access to Certificates, CRLs and ARLs)	Username/pwd
Via Internet		
SMKI Portal via Internet (Org Certs)	Authentication to SMKI Portal via Internet (manual submission of Organisation CSRs)	IKI Certificate
File-Signing		
Threshold Anomaly Detection / Central Products list, etc	Digital Signing of ADT files, the CPL or communications related to the SMKI Recovery Procedures.	IKI Certificate

Figure 1: Overview of SMKI access registration processes

- SMKI RAPP Section 5.1 sets out the procedure and detailed processes for confirming the role of the nominating individual and verifying the organisational identity of the Party, RDP, Manufacturer, SECCo or DCC Service Provider, which shall be conducted where its identity has not previously been established.

- SMKI RAPP Section 5.2 sets out the procedure and detailed processes for verifying the identity of an individual nominated to become an SRO. The DCC shall ensure that an individual cannot become an SRO until the organisational identity of the applicant has been verified.

- SMKI RAPP Section 5.3 sets out the procedure and detailed processes for verifying the identity of an individual nominated to become an ARO. The DCC shall ensure that an individual cannot become an ARO until the organisation has at least one SRO and the organisational identity of the applicant has been verified.

- Once an individual has become an ARO, SMKI RAPP Section 5.4 sets out the procedure and detailed processes by which the appropriate credentials used to access SMKI Services and/or the SMKI Repository Service are provided to AROs.

- Where an applicant wishes to be an Authorised Subscriber for Organisation Certificates or Device Certificates or both, Section 5.5 of the SMKI RAPP sets out the procedure and detailed processes by which the DCC determines if the applicant is eligible to become an Authorised Subscriber for such Organisation Certificates or Device Certificates or both.

In respect of the procedures and detailed processes set out in SMKI RAPP Sections 5.1 to 5.5, the DCC shall place no restriction on the number of forms that can be submitted by an individual Party, RDP, Manufacturer, SECCo or the DCC. Where reasonably practicable, the DCC shall conduct the procedures as set out in SMKI RAPP Sections 5.1 to 5.5 such that where multiple forms are submitted at the same time, multiple procedures can be conducted via a video link by the applicant's nominated individuals.

4.1.3 Change of details

If there is a change to any of the information used to verify the organisational identity of any Party, RDP, Manufacturer, SECCo or a DCC Service Provider (acting on behalf of the DCC), an SRO shall advise the Service Desk of the change and shall ensure that the procedure and detailed processes as set out in SMKI RAPP Section 5.1 is undertaken in respect of the revised evidence of identity, as soon as is reasonably practicable after the change occurs.

If there is a material change to any of the information used to verify the identity of any SRO or ARO, an SRO shall:

a) advise the Service Desk of the change;

b) where required to do so by the SMKI Registration Authority, check the name and address of an ARO before issuing a replacement token, ensure that its SRO or ARO undertakes the procedures as set out in SMKI RAPP Sections 5.2 or 5.3 in respect of the revised evidence of identity, as soon as is reasonably practicable after a material change occurs; and

c) where necessary, for an ARO ensure that credentials used to access SMKI Services and/or the SMKI Repository Service are revoked as set out in SMKI RAPP Section 8.3.

No Party, RDP, Manufacturer, SECCo or the DCC (acting as DCC Service Provider) shall unreasonably withhold information that is required by the SMKI Registration Authority in order to perform the procedures as set out in SMKI RAPP Sections 5.1 to 5.5.

4.1.4 Director or Company Secretary ceasing to be eligible to act on behalf of a Party, RDP, Manufacturer or SECCo

Where Director or Company Secretary ceases to be eligible to act on behalf of a Party, RDP, Manufacturer or SECCo in respect of the procedures set out in the SMKI RAPP:

a) the Director or Company Secretary themselves, or a Senior Responsible Officer (SRO) whose identity has previously been verified by the DCC, shall advise the Service Desk of the change;

b) the DCC shall confirm such information from the relevant Nominee Details Form, in order to provide confidence that the request is from a Director, Company Secretary or SRO; and

c) if b) is successful, the DCC shall update the DCC’s records of authorised individuals for the Party, RDP, Manufacturer or SECCo and shall no longer consider the individual to be able to act on behalf of that Party, RDP, Manufacturer or SECCo.

4.1.5 SROs ceasing to be eligible to act on behalf of a Party, RDP, Manufacturer or SECCo

Where an SRO ceases to be eligible to act on behalf of a Party, RDP, Manufacturer or SECCo in respect of the procedures set out in the SMKI RAPP:

a) the SRO themselves, or a Director, Company Secretary or SRO whose identity has previously been verified by the DCC, shall advise the Service Desk of the change;

b) the DCC shall confirm such information from the relevant Nominee Details Form, in order to provide confidence that the request is from an SRO, Director or Company Secretary; and

c) if b) is successful, update the DCC's records of authorised individuals for the Party, RDP, Manufacturer or SECCo and shall no longer consider the individual to be able to act on behalf of that Party, RDP, Manufacturer or SECCo.

5. Detailed Party, RDP, Manufacturer, SECCo and DCC (as DCC Service Provider) registration procedures and processes

Each Party, RDP, Manufacturer, SECCo and DCC (in its role as DCC Service Provider) shall ensure that its nominated representatives wishing to access SMKI Services and/or the SMKI Repository Service shall undertake the procedures and processes as set out in SMKI RAPP Sections 5.1 to 5.5, as appropriate.

5.1 Procedure and processes to verify organisational identity

The processes as detailed immediately below shall be conducted by the SMKI Registration Authority in order to verify the organisational identity of a Party, RDP, Manufacturer, SECCo or DCC Service Provider (acting on behalf of the DCC).

Step	When	Obligation	Responsibility	Next Step
5.1.1	As required	The applicant organisation shall complete the Organisation Information Form, as set out in SMKI RAPP Annex A (A1). In doing so, the applicant organisation shall ensure that: a. the information entered on the form is complete and accurate; b. the EUI-64 Compliant identifier range for any particular User Role is defined by the applicant organisation such that the range is continuous and does not overlap with	Director or Company Secretary, on behalf of the applicant organisation, which shall be a Party, RDP, Manufacturer, SECCo or DCC Service Provider	5.1.2

		the EUI-64 Compliant identifier range for any other User Role, other than where a particular EUI-64 Compliant identifier is allowed to be used for more than one User Role in accordance with H1.5; and c. the Organisation Information Form is authorised by a Director or Company Secretary on behalf of the applicant organisation. The applicant organisation shall also complete the Nominee Details Form, as set out in SMKI RAPP Annex A (A5), for the Director or Company Secretary that has authorised the Organisation Information Form. In doing so, the applicant organisation shall ensure that the information entered on the form is complete and accurate.		
5.1.2	As required, following 5.1.1	Submit the completed Organisation Information Form and Nominee Details Form to the SMKI Registration Authority,	Director or Company Secretary, on behalf of the applicant organisation,	5.1.3

		in writing, as directed on the DCC Website.	which shall be a Party, RDP, Manufacturer, SECCo or DCC Service Provider	
5.1.3	As soon as reasonably practicable following receipt of completed Organisation Information Form	Acknowledge receipt by email to the Director or Company Secretary that has authorised the Organisation Information Form.	Service Desk	5.1.4
5.1.4	As soon as reasonably practicable following 5.1.3	Confirm that the nominating Director or Company Secretary holds such a position within the application organisation, via a public information source. Analyse the information entered on the Organisation Information Form and Nominee Details Form, to determine completeness, discrepancies and whether the submitted EUI-64 Compliant identifier ranges are consistent with the restriction set out in step 5.1.1. Where there are omissions/discrepancies or the submitted identifier ranges are not consistent with the restriction set out in step 5.1.1, the SMKI Registration Authority shall agree actions and/or amendments, via email, with the Director or Company Secretary that has authorised the Organisation Information Form.	SMKI Registration Authority Personnel	If complete, accurate and no discrepancies, 5.1.6; if not complete and accurate or any discrepancies, 5.1.5
5.1.5	Once omissions / discrepancies addressed	Submit a revised Organisation Information Form and/or Nominee Details Form to the SMKI Registration Authority, or in writing as directed on the DCC Website.	Director or Company Secretary, on behalf of the applicant organisation, which shall be a Party, RDP, Manufacturer, SECCo or DCC Service Provider	5.1.3

5.1.6	As soon as reasonably practicable, following 5.1.4	Agree with the applicant organisation and confirm, by email, the date and time of a meeting to verify the organisation identity to the Director, or Company Secretary that has signed the Organisation Information Form. The meeting shall be held via a video link or face to face if preferred.	SMKI Registration Authority	5.1.7
5.1.7	As soon as reasonably practicable on becoming aware of unavailability	If it is identified that SMKI Registration Authority Personnel will be unavailable to conduct the verification meeting on the agreed date and time, the SMKI Registration Authority shall inform the applicant Director or Company Secretary by email, and shall agree and confirm an alternative date and time. If it is identified that the individual(s) acting on behalf of the applicant organisation will be unavailable to attend the verification meeting on the agreed date and time, the individual(s) shall inform the SMKI Registration Authority, by email, and shall agree and confirm an alternative date and time.	SMKI Registration Authority or applicant organisation, as appropriate	5.1.8
5.1.8	In meeting to verify organisational identity	Verify: a. the organisational identity of the applicant organisation to the level pursuant to the SMKI PMA Guidance on "Verifying Organisation Identity" published on the Website; b. via information held by SECCo, that the applicant organisation has the User Role or User Roles as specified in Organisation Information Form; c. proof of individual identity provided for the nominating individual against the information listed on the Organisation Information Form and the Nominee Details Form; and d. the individual identity of the nominating individual to the level pursuant to the SMKI PMA Guidance on "Verifying Individual Identity" published on the Website.	SMKI Registration Authority Personnel	If not successful, 5.1.9; if successful, 5.1.10
5.1.9	As soon as reasonably practicable, following 5.1.8	If verification in 5.1.8 is unsuccessful, notify the nominating Director, Company Secretary or SRO that verification of the organisational identity has been unsuccessful, by email.	SMKI Registration Authority Personnel	5.1.5 once issues addressed

5.1.10	As soon as reasonably practicable, following 5.1.8	If verification in 5.1.8 is successful, inform the nominating Director or Company Secretary that the organisational identity has been successfully verified, by email.	SMKI Registration Authority	5.1.11
5.1.11	As soon as reasonably practicable, following 5.1.10	Add the verified organisation to the DCC's list of such organisations, in accordance with Section 4.1.2 (A) (ii) of Appendix A to the Code and Section 4.1.2 (A) (ii) of Appendix B to the Code.	SMKI Registration Authority	End of procedure

5.2 Procedure for becoming a Senior Responsible Officer

The procedure as detailed immediately below shall be conducted by the SMKI Registration Authority in order to check the authorisation and verify the identity of any individual that has been nominated to become a Senior Responsible Officer in respect of that Party, RDP, Manufacturer, SECCo or the DCC (in its role as DCC Service Provider).

Step	When	Obligation	Responsibility	Next Step
5.2.1	As required	Complete the SMKI SRO Nomination Form and Nominee Details Form, as set out in SMKI RAPP Annex A (A3) and Annex A (A5). In doing so, the individual completing the SMKI SRO Nomination Form and Nominee Details Form shall ensure that the information entered on the forms is complete and accurate, and that: a. the nominating individual is for a Party, RDP, Manufacturer, SECCo or the DCC (as DCC Service Provider), a Director of, or Company Secretary of and an employee of, the applicant organisation or its parent organisation; and b. the SMKI SRO Nomination Form and Nominee Details Form are both authorised, where applicable, by a Director or Company Secretary on behalf of the applicant organisation.	Director or Company Secretary, on behalf of the applicant organisation, which shall be a Party, RDP, Manufacturer, SECCo or DCC (as DCC Service Provider).	5.2.2
5.2.2	As required, following 5.2.1	Submit the completed SMKI SRO Nomination Form and Nominee Details Form to the SMKI Registration Authority, in writing, as	Director or Company Secretary, on behalf of the applicant organisation,	5.2.3

		directed on the DCC Website.	which shall be a Party, RDP, Manufacturer, SECCo or DCC (as DCC Service Provider).	
5.2.3	As soon as reasonably practicable following receipt of completed SRO Nomination Form	Acknowledge receipt to the Director or Company Secretary that has authorised the SMKI SRO Nomination Form.	Service Desk	5.2.4
5.2.4	As soon as reasonably practicable following 5.2.3	Analyse the information entered on the SMKI SRO Nomination Form and Nominee Details Form, to: a. determine completeness and any discrepancies; and b. confirm, using the DCC's records or using publicly available information, that the Director or Company Secretary that has authorised the SMKI SRO Nomination Form has the role indicated on the SMKI SRO Nomination Form. Where there are omissions/discrepancies, agree actions with the nominating individual, via email.	SMKI Registration Authority Personnel	If complete, 5.2.6; if not complete, 5.2.5
5.2.5	Once omissions / discrepancies addressed	Submit a revised SMKI SRO Nomination Form and/or Nominee Details Form to the SMKI Registration Authority, in writing as directed on the DCC Website.	Director or Company Secretary, on behalf of the applicant organisation, which shall be a Party, RDP, Manufacturer, SECCo or DCC (as DCC Service Provider).	5.2.3

5.2.6	As soon as reasonably practicable, following 5.2.4	If the SMKI Registration Authority has any questions about the information submitted, contact the Director or Company Secretary that nominated the individual, via telephone, using the telephone number provided previously in the SMKI SRO Nomination Form, to confirm whether each nominated individual on the SMKI SRO Nomination Form is authorised to act on behalf of the organisation as SRO and seek confirmation of information provided on the SMKI SRO Nomination Form in order to provide confidence that the correct person has been contacted.	SMKI Registration Authority Personnel	If confirmed as authorised, 5.2.8; if not confirmed as authorised, 5.2.7
5.2.7	As soon as reasonably practicable following rejection	Inform the applicant organisation that the application to become a Senior Responsible Officer has not been successful, by email to the Director or Company Secretary that has authorised the SMKI SRO Nomination Form.	SMKI Registration Authority Personnel	5.2.6 once issues resolved
5.2.8	As soon as reasonably practicable, following 5.2.6	Agree, via email with the individual nominated to become a Senior Responsible Officer, a date and time for the nominated individual(s) to attend a face to face verification meeting in person or by video link.	SMKI Registration Authority Personnel	5.2.9
5.2.9	As soon as reasonably practicable on becoming aware of unavailability	If it is identified that SMKI Registration Authority Personnel will be unavailable to conduct the verification meeting on the agreed date and time, the SMKI Registration Authority shall inform the nominated individual, and shall agree and confirm an alternative date and time. If it is identified that the individual(s) nominated to act on behalf of the applicant organisation will be unavailable to attend the verification meeting on the agreed date and time, the nominated individual shall inform the SMKI Registration Authority, by email and telephone, and shall agree and confirm an alternative date and time.	SMKI Registration Authority or applicant organisation, as appropriate	5.2.10
5.2.10	In SRO verification meeting	At the face-to-face SRO verification meeting in person or by video link, the SMKI Registration Authority shall, in person: a. check proof of individual identity provided for each nominated individual against the information listed on the SRO Nomination Form and the	SMKI Registration Authority	If not successfully verified, 5.2.11; if successfully verified, 5.2.12

		Nominee Details Form; and b. verify the individual identity for each nominated individual to the level pursuant to the SMKI PMA Guidance on "Verifying Individual Identity" published on the Website.		
5.2.11	As soon as reasonably practicable, following verification meeting	Notify the Director or Company Secretary in writing, that the nominated individual(s) has not been verified successfully and has not become a Senior Responsible Officer on behalf of the applicant organisation.	SMKI Registration Authority	5.2.5 once issues addressed
5.2.12	As soon as reasonably practicable, following verification meeting	Notify the Director or Company Secretary in writing, that the nominated individual(s) has become a Senior Responsible Officer on behalf of the applicant organisation.	SMKI Registration Authority	5.2.13
5.2.13	As soon as reasonably practicable, 5.2.12	Add the relevant SRO to the DCC's list of SROs, in accordance with Section 4.1.2 (A) (ii) of Appendix A to the Code and Section 4.1.2 (A) (ii) of Appendix B to the Code.	SMKI Registration Authority	End of Procedure

5.3 Procedure for becoming an Authorised Responsible Officer

The procedure as detailed immediately below shall be conducted by the SMKI Registration Authority in order to check the authorisation and verify the identity of any individual that has been nominated to become an Authorised Responsible Officer in respect of that Party, RDP, Manufacturer, SECCo or the DCC (in its role as DCC Service Provider).

Step	When	Obligation	Responsibility	Next Step
5.3.1	As required	Complete the SMKI ARO Nomination Form and Nominee Details Form as set out in SMKI RAPP Annex A (A4) and Annex A (A5), ensuring that; a. the information entered on the forms is complete and	SRO on behalf of the applicant organisation, which shall be a Party, RDP, Manufacturer, SECCo or DCC (as DCC Service Provider)	5.3.2

		accurate; b. the SMKI ARO Nomination Form and Nominee Details Form are authorised by an SRO on behalf of the applicant organisation; and c. the SRO has confirmed that the SMKI ARO Nominee has been subject to a standard that is compliant with BS 7858:2019 or an equivalent standard.		

5.3.2	As required, following 5.3.1	Submit the completed SMKI ARO Nomination Form and Nominee Details Form to the SMKI Registration Authority in writing, as directed on the DCC Website.	SRO on behalf of the applicant organisation, which shall be a Party, RDP, Manufacturer, SECCo or DCC (as DCC Service Provider)	5.3.3

5.3.3	As soon as reasonably practicable following receipt of completed ARO Nomination Form and Nominee Details Form	Acknowledge receipt by email to the SRO as identified on the SMKI ARO Nomination Form.	Service Desk	5.3.4

5.3.4	As soon as reasonably	Analyse the information entered on the SMKI ARO Nomination Form and Nominee Details	SMKI Registration Authority	If complete,

	practicable following 5.3.3	Form; determine completeness and any discrepancies. Where there are omissions/discrepancies, agree actions with the SRO via email.		5.3.6; if not complete, 5.3.5
5.3.5	Once omissions / discrepancies are addressed	Submit a revised SMKI ARO Nomination Form and/or Nominee Details Form to the Registration Authority in writing as directed on the DCC Website.	SRO on behalf of the applicant organisation, which shall be a Party, RDP, Manufacturer, SECCo or DCC (as DCC Service Provider)	5.3.3
5.3.6	As soon as reasonably practicable, following 5.3.4	If the SMKI Registration Authority has any questions about the information submitted, contact an SRO of the applicant organisation via telephone, using the registered contact information for the SRO as held by the SMKI Registration Authority, to confirm whether the nominated individual is authorised to become an ARO.	SMKI Registration Authority	If confirmed as authorised, 5.3.8; if not authorised, 5.3.7
5.3.7	As soon as reasonably practicable following rejection	Notify the individual and an SRO that the procedure for becoming an ARO has not been successful for relevant nominated individual, by email.	SMKI Registration Authority	5.3.5 once issues addressed
5.3.8	As soon as reasonably practicable, following 5.3.6	Agree with the applicant organisation and confirm the date and time for the ARO verification meeting, via email to the nominated individual and an SRO of the applicant organisation.	SMKI Registration Authority	5.3.9
5.3.9	As soon as reasonably practicable on becoming aware of unavailability	If it is identified that SMKI Registration Authority Personnel will be unavailable to conduct the verification meeting on the agreed date and time, the SMKI Registration Authority shall inform an SRO and the nominated individual, by email, and shall agree and confirm an alternative date and time. If it is identified that the nominated individual(s) acting on behalf of the applicant organisation will be unavailable to attend the verification meeting on the agreed date and time, an SRO shall inform the SMKI Registration Authority, by	SMKI Registration Authority or applicant organisation, as appropriate	5.3.10

		email, and shall agree and confirm an alternative date and time.		
5.3.10	In ARO verification meeting	At the ARO face-to-face verification meeting, the SMKI Registration Authority shall, in person, for the nominated individual: a. check proof of individual identity provided against the information listed on the ARO Nomination Form and Nominee Details Form; and b. verify the identity of the nominated individual to the level pursuant to the SMKI PMA Guidance on "Verifying Individual Identity" published on the Website.	SMKI Registration Authority	If verified, 5.3.12; if not verified, 5.3.11
5.3.11	As soon as reasonably practicable, following ARO verification meeting	Notify: a. the nominated individual that they have become an ARO, verbally; or b. in writing to the SRO, that the verification has not been successful for the nominated individual, that the nominated individual has not become an ARO, and provide reasons for the rejection and request that the nominated individual is required to attend a further ARO verification meeting once the issues have been remedied.	SMKI Registration Authority	If successful, 5.3.12; otherwise 5.3.5 once issues are addressed
5.3.12	As soon as reasonably practicable, following ARO verification meeting	Ensure that the applicant organisation is notified of the individuals whose identity has been verified and have become AROs by email or via the Service Desk updating the relevant ticket, ensuring that there is a record for audit purposes.	SMKI Registration Authority or Service Desk	5.3.13
5.3.13	As soon as reasonably practicable, following 5.3.12	Add the relevant individual to the DCC's list of AROs, in accordance with Section 4.1.2 (A) (ii) of Appendix A to the Code and Section 4.1.2 (A) (ii) of Appendix B to the Code.	SMKI Registration Authority	Procedure as set out in SMKI RAPP section 5.5

5.4 Procedure for provision of credentials to AROs for accessing SMKI Services and the SMKI Repository Service and file signing

The procedure and processes as detailed immediately below shall be conducted by the SMKI Registration Authority in order to provide credentials for accessing SMKI Services and/or the SMKI Repository Service or for file signing to Authorised Responsible Officers in respect of a Party, RDP, Manufacturer, SECCo or the DCC (in its role as DCC Service Provider). The SMKI Registration Authority shall not provide such credentials to an individual on behalf of a Party, RDP, Manufacturer, SECCo or the DCC (in its role as DCC Service Provider), other than where the organisation has completed SMKI and Repository Entry Process Tests and such individuals have become Authorised Responsible Officers.

Step	When	Obligation	Responsibility	Next Step
5.4.1	During ARO verification meeting and after becoming an ARO	**IKI credentials for submission of CSRs in respect of Organistion Certificates using SMKI Portal via DCC Gateway Connection or SMKI Portal via the Internet** If the applicant has indicated on the Authorised Subscriber application form that it wishes to be an Authorised Subscriber for Organisation Certificates and/or Device Certificates, and where the Party, RDP, Manufacturer, SECCo or DCC Service Provider has successfully completed SMKI and Repository Entry Process Tests, the SMKI Registration Authority shall, if the ARO wishes to access the SMKI Portal interface, provide the ARO with: a. If the	SMKI Registration Authority	5.4.2

		applicant organisation has access to a DCC Gateway Connection, one Cryptographic Credential Token containing credentials issued under the applicable IKI Certification Authority that authenticate the ARO to access the SMKI Portal Interface for the purposes of submission of CSRs in respect of Organisation Certificates and retrieval of corresponding Organisation Certificates via a DCC Gateway Connection. The DCC shall ensure that the Cryptographic Credential Token enables the ARO to set a PIN code which shall be used each		

		time the Cryptographic Credential Token is used, to render the Cryptographic Credential Token operative. Such credentials shall not allow the ARO to access the SMKI Portal Interface via the Internet. b. If the applicant organisation does not have access to a DCC Gateway Connection, one Cryptographic Credential Token containing credentials issued under the applicable IKI Certification Authority that authenticate the ARO to access the SMKI Portal Interface via the Internet for the purposes of submission of CSRs in respect of		

		Organisation Certificates and retrieval of corresponding Organisation Certificates. The DCC shall ensure that the Cryptographic Credential Token enables the ARO to set a PIN code which shall be used each time the Cryptographic Credential Token is used, to render the Cryptographic Credential Token operative. Such credentials shall not allow the ARO to access the SMKI Portal Interface via a DCC Gateway Connection. Where the Party, RDP, Manufacturer, SECCo or DCC (in its role as DCC Service Provider) has not successfully completed SMKI and Repository Entry Process Tests, the DCC shall retain such		

		Cryptographic Credential Token until such time as the Party, RDP, Manufacturer, SECCo or DCC (as DCC Service Provider) has successfully completed SMKI and Repository Entry Process Tests, at which point the DCC shall send such Cryptographic Credential Token to the ARO via secure courier.		

5.4.2	During ARO verification meeting and after becoming an ARO	**IKI credentials for submission of CSRs in respect of Device Certificates using SMKI Portal via DCC Gateway Connection** If the applicant has indicated on the Authorised Subscriber application form that it wishes to be an Authorised Subscriber for Device Certificates, the Registration Authority shall determine, in accordance with the steps set out in Section 5.5 of the SMKI RAPP, whether there is reasonable evidence to suggest that it is necessary for the applicant organisation to become an Authorised Subscriber for Device Certificates in order for them to carry out business processes that will, or are likely to, lead to the installation of Devices in premises. Where there is such reasonable evidence, and where the applicant organisation has successfully completed SMKI and Repository Entry Process Tests, the SMKI Registration Authority shall, if the ARO wishes to access the SMKI Portal Interface, provide the ARO with: a. If the applicant organisation has access to a DCC Gateway Connection, one Cryptographic Credential Token containing credentials issued under the applicable IKI Certification Authority that authenticate the ARO to access the SMKI Portal Interface for the purposes of submission of CSRs in respect of Device Certificates and retrieval of corresponding Device Certificates via a DCC Gateway Connection. The DCC shall ensure that the Cryptographic	SMKI Registration Authority	5.4.3

		Credential Token enables the ARO to set a PIN code which shall be used each time the Cryptographic Credential Token is used, to render the Cryptographic Credential Token operative. Such credentials shall not allow the ARO to access the SMKI Portal Interface via the Internet. Where the Party, RDP or DCC (in its role as DCC Service Provider) has not successfully completed SMKI and Repository Entry Process Tests, the DCC shall retain such Cryptographic Credential Token until such time as the Party, RDP or DCC (as DCC Service Provider) has successfully completed SMKI and Repository Entry Process Tests, at which point the DCC shall send such Cryptographic Credential Token to the ARO via secure courier.		

5.4.3	During ARO verification meeting and after becoming an ARO	**IKI credentials for Ad Hoc Device CSR Web Service** If the applicant has indicated on the Authorised Subscriber application form that it wishes to be an Authorised Subscriber for Device Certificates and it wishes to use the Ad Hoc Device CSR Web Service, the SMKI Registration Authority shall, if the applicant organisation has access to a DCC Gateway Connection and is a Supplier Party or the DCC, and where the Supplier Party or DCC (in its role as DCC Service Provider) has successfully completed SMKI and Repository Entry Process Tests, the SMKI Registration Authority shall provide the ARO, via USB token or optical media, with Ad Hoc Device CSR Web Service access credentials for Device Certificates, which corresponds with a CSR that shall be provided, via USB token or optical media, by the applicant organisation in accordance with the SMKI Interface Design Specification, sections 2.4 xv, xvi & xvii. If the Supplier Party or DCC (in its role as DCC Service Provider) has not successfully completed SMKI and Repository Entry Process Tests at the time of the verification meeting, once the Supplier Party or DCC (as DCC Service Provider) has successfully completed SMKI and Repository Entry Process Tests, the SMKI Registration Authority shall provide, on a USB token or optical media via secure courier or by secured electronic means, the appointed ARO with Ad	SMKI Registration Authority	5.4.4

		Hoc Device CSR Web Service access credentials for Device Certificates, which corresponds with a CSR that shall be provided by the applicant organisation in accordance with the SMKI Interface Design Specification.		
5.4.4	During ARO verification meeting and after becoming an ARO	**IKI credentials for Batched Device CSR Web Service** If the applicant has indicated on the Authorised Subscriber application form that it wishes to be an Authorised Subscriber for Device Certificates and it wishes to use the Batched Device CSR Web Service, the SMKI Registration Authority shall determine, if the applicant organistaion has access to a DCC Gateway Connection and the applicant is not a Supplier Party or the DCC, in accordance with the steps set out in Section 5.5 of the SMKI RAPP, whether there is reasonable evidence to suggest that it is necessary for the applicant organisation to become an Authorised Subscriber for Device Certificates in order for them to carry out business processes that will, or are likely to, lead to the installation of Devices in premises. Where there is such reasonable evidence, and where the applicant organisation has successfully completed SMKI and Repository Entry Process Tests, the SMKI Registration Authority shall provide the appointed ARO, via USB token or optical media, with Batched Device CSR Web Service access credentials for Device Certificates, which shall be Issued by the DCC in response to a valid CSR that shall be provided by the applicant organisation in accordance with the SMKI Interface Design Specification, sections 2.5 xxvi & xxvii. If the applicant organisation has not successfully completed SMKI and Repository Entry Process Tests at the time of the verification meeting, once the applicant organisation has successfully completed SMKI and Repository Entry Process Tests, the SMKI Registration Authority shall provide, on a USB token or optical media via secure courier or by secured electronic means, the appointed ARO with Batched Device CSR Web Service access credentials for Device Certificates, which corresponds with a CSR that shall be provided by the applicant organisation in accordance with the SMKI Interface Design Specification.	SMKI Registration Authority	5.4.5

5.4.5	During ARO verification meeting and after becoming an ARO	**Credentials for SMKI Repository portal** If the applicant organisation has access to a DCC Gateway Connection, and it wishes to access the SMKI Repository via the SMKI Repository Portal and has successfully completed SMKI and Repository Entry Process Tests, provide the appointed ARO with a username and password, to be accessed via the SMKI Repository Portal, that is specific to the Authorised Responsible Officer, for the purposes of authenticating to the SMKI Repository Portal via DCC Gateway Connection, as set out in the SMKI Repository Interface Design Specification, section 2.1.2. If the applicant organisation has access to a DCC Gateway Connection, it wishes to access the SMKI Repository via the SMKI Repository Portal but has not successfully completed SMKI and Repository Entry Process Tests at the time of the verification meeting: a. DCC shall, once the applicant organisation has successfully completed SMKI and Repository Entry Process Tests, provide the appointed ARO with a username and password via secured electronic means that is specific to the Authorised Responsible Officer, for the purposes of authenticating to the SMKI Repository Portal via DCC Gateway Connection, as set out in the SMKI Repository Interface Design Specification, section 2.1.2.	SMKI Registration Authority	5.4.6

5.4.6	During ARO verification meeting and after becoming an ARO	**Credentials for SMKI Repository web service** If the applicant organisation has access to a DCC Gateway Connection, and wishes to access the SMKI Repository Web Service interface and has successfully completed SMKI and Repository Entry Process Tests, provide the ARO with the credentials required to authenticate to the SMKI Repository Web Service interface, as set out in the SMKI Repository Interface Specification section 2.2.1, along with a certificate which enables verification of the SMKI Repository Web Service server identity. If the applicant organisation has access to a DCC Gateway Connection, wishes to access the SMKI Repository Web Service interface but has not successfully completed SMKI and Repository Entry Process Tests at the time of the	SMKI Registration Authority	5.4.7

		verification meeting, once the applicant organisation has successfully completed SMKI and Repository Entry Process Tests, the SMKI Registration Authority shall provide, on electronic media as set out in the "SMKI Repository User Guide", the ARO with the credentials required to authenticate to the SMKI Repository Web Service interface, as set out in the SMKI Repository Interface Design Specification section 2.2.1.		
5.4.7	During ARO verification meeting and after becoming an ARO	**Credentials for SMKI Repository Portal SFTP** If the applicant organisation has access to a DCC Gateway Connection, wishes to access the SMKI Repository using SSH File Transfer Protocol (SFTP) access credentials and has successfully completed SMKI and Repository Entry Process Tests, provide the ARO with credentials, in the form of a username and password, used to access the SSH File Transfer Protocol (SFTP) interface, as set out in the SMKI Repository Interface Design Specification section 2.3.1. If the applicant organisation has access to a DCC Gateway Connection, wishes to access the SMKI Repository using SSH File Transfer Protocol (SFTP) access credentials but has not successfully completed SMKI and Repository Entry Process Tests at the time of the verification meeting, once the applicant organisation has successfully completed SMKI and Repository Entry Process Tests, the SMKI Registration Authority shall provide the ARO, via the SMKI Repository Portal profile page, with credentials, in the form of a username and password, used to access the SSH File Transfer Protocol (SFTP) interface, as set out in the SMKI Repository Interface Design Specification section 2.3.1.	SMKI Registration Authority	5.4.8
5.4.8	During ARO verification meeting and after becoming an ARO	**IKI credentials for file signing** If the applicant organisation wishes the ARO to be Issued with a File Signing Certificate for the purposes as set out in the Code, the SMKI Registration Authority shall either: a. provide the ARO with a Cryptographic Credential Token enabling the ARO to submit a CSR for a File Signing Certificate; in which case, the ARO shall use the software on the Cryptographic	SMKI Registration Authority	5.4.9

		Credential Token to generate a Private Key for a File Signing Certificate to submit a CSR for a File Signing Certificate; and if the CSR is valid, the ICA shall Issue a File Signing Certificate under the IKI Certificate Policy, to be used for the purposes as set out in the Code; or b. provide the appointed ARO, via USB token or optical media, with an IKI File Signing Certificate, which shall be Issued by the DCC in response to a valid CSR that shall be provided by the applicant organisation.		
5.4.9	During ARO verification meeting and after issuance of credentials	**Acceptance of credentials issued in steps 5.4.1 to 5.4.8** The SMKI Registration Authority shall complete the relevant sections of the Nominee Details Form in Annex A (A5) accordingly to confirm credential issuance either manually or digitally and give the form to the ARO, retaining a copy of the original. The ARO shall confirm receipt of and acceptance of the credentials issued by completing the relevant sections of the Nominee Details Form in Annex A (A5) either manually or digitally. The SMKI Registration Authority shall retain a copy of the receipt. Should the ARO not wish to accept these credentials, the ARO shall notify the SMKI Registration Authority immediately and not sign for the Certificate and / or Cryptographic Credential.	SMKI Registration Authority ARO	End of procedure

5.5 Procedure for becoming an Authorised Subscriber

An organisation is an Authorised Subscriber for IKI File Signing Certificates where it has successfully appointed and maintains in place at least one SRO and at least one ARO.

The procedure detailed immediately below shall be conducted by the DCC, in order to determine whether a Party, RDP or the DCC (in its role as DCC Service Provider) has become an Authorised Subscriber for Organisation Certificates, an Authorised Subscriber for Device Certificates, or both.

Step	When	Obligation	Responsibility	Next Step
5.5.1	As required	Complete the Authorised Subscriber / Interface Access Application Form as set out in SMKI	SRO on behalf of the applicant	5.5.2

		RAPP Annex A (A2), ensuring that the information entered on the form is complete and accurate, and the Authorised Subscriber Application Form is authorised by an SRO on behalf of the applicant organisation.	organisation, which shall be a Party, RDP or the DCC (in its role as DCC Service Provider)	
5.5.2	As required, following 5.5.1	Submit the completed Authorised Subscriber Application Form to the SMKI Registration Authority in writing, as directed on the DCC Website.	Applicant organisation, which shall be a Party or RDP	5.5.3
5.5.3	As soon as reasonably practicable following 5.5.2	Acknowledge receipt by email to the SRO as identified on the Authorised Subscriber / Interface Access Application Form.	SMKI Registration Authority	5.5.4
5.5.4	As soon as reasonably practicable following 5.5.3	Analyse the information entered on the Authorised Subscriber / Interface Access Application Form; determine completeness and any discrepancies. Where there are omissions/discrepancies, agree actions with an SRO via email.	SMKI Registration Authority	If complete, 5.5.6; if not complete, 5.5.5
5.5.5	Once omissions / discrepancies are addressed	Submit a revised Authorised Subscriber / Interface Access Application Form to the SMKI Registration Authority in writing, as directed on the DCC Website.	SRO on behalf of the applicant organisation, which shall be a Party, RDP or the DCC (in its role as DCC Service Provider)	5.5.3
5.5.6	As soon as reasonably practicable, following 5.5.4	Contact the SRO as identified on the Authorised Subscriber / Interface Access Application Form via telephone, using the registered contact information for the SRO as held by the SMKI Registration Authority. The SMKI Registration Authority shall verbally confirm details for the SRO as held by the DCC to verify that the correct individual has been contacted. The SMKI Registration Authority shall confirm the applications indicated on the Authorised Subscriber / Interface Access Application Form are authorised.	SMKI Registration Authority	If confirmed as authorised, 5.5.8; if not authorised, 5.5.7

5.5.7	As soon as reasonably practicable following rejection	Notify the SRO as identified on the Authorised Subscriber / Interface Access Application Form that the procedure in respect of the application has not been successful, in writing.	SMKI Registration Authority	5.5.5 once issues addressed
5.5.8	As requested	Where the application organisation is not a DCC Service Provider, conduct the SMKI and Repository Entry Process Tests if SMKI and Repository Entry Process Tests have not been completed previously, in accordance with Sections H14.22 to H14.30 of the Code.	Applicant organisation, in respect of the corresponding Authorised Subscriber / Interface Access Application Form	If successful or the applicant organisation is a DCC Service Provider (acting on behalf of the DCC), 5.5.10; if not successful, 5.5.9
5.5.9	As soon as reasonably practicable, following 5.5.8	The DCC shall confirm in writing, to the SRO as identified on the Authorised Subscriber / Interface Application Form, that the SMKI and Repository Entry Process Tests were not completed successfully.	DCC	5.5.8 once issues addressed
5.5.10	As soon as reasonably practicable, following 5.5.8	The DCC shall confirm in writing to the relevant Party that the SMKI and Repository Entry Process Tests have been completed successfully.	DCC	5.5.11
5.5.11	As soon as reasonably practicable, following 5.5.10	If the applicant organisation has indicated on its Authorised Subscriber / Interface Access Application Form that it wishes to become an Authorised Subscriber in respect of the Organisation Certificate Policy, the SMKI Registration Authority shall confirm in writing to the SRO as identified on the Authorised Subscriber / Interface Access Application Form that it the applicant organisation has become an Authorised Subscriber for Organisation Certificates. Where appropriate, the DCC shall issue credentials enabling the applicant to act as an Authorised Subscriber for Organisation Certificates, in accordance with the procedural steps as set out in section 5.4 of this document.	SMKI Registration Authority	If the applicant organisation has indicated that it wishes to become an Authorised Subscriber for Device Certificates, 5.5.12; otherwise, 5.5.17

5.5.12	As soon as possible, following 5.5.11	If the applicant organisation has indicated on the Authorised Subscriber / Interface Access Application Form that it wishes to become an Authorised Subscriber in respect of the Device Certificate Policy, the SMKI Registration Authority shall assess whether there is evidence to confirm that the Party has completed the User Entry Process (defined in Section H1.10) and will use a DCC Gateway Connection to obtain Device Certificates.	SMKI Registration Authority	If determined to be an Authorised Subscriber for Device Certificates, 5.5.15; otherwise 5.5.13
5.5.13	As soon as possible, following 5.5.12	Confirm by email, to the SRO as identified on the Authorised Subscriber / Interface Access Application Form, that the DCC has determined that applicant organisation is not eligible to become an Authorised Subscriber for Device Certificates.	SMKI Registration Authority	5.5.14
5.5.14	As soon as possible, following 5.5.13	In the case of a dispute by the SRO where the DCC has determined that there is no evidence as defined in 5.5.12 to support the applicant organisation to become such an Authorised Subscriber, the DCC shall notify the SMKI PMA of the refusal.	SMKI Registration Authority	End of procedure
5.5.15	As soon as reasonably practicable, following 5.5.12, or, where a Supplier Party or the DCC (in its role as DCC Service Provider) has indicated that it wishes to become an Authorised Subscriber in respect of the Device Certificate Policy	The SMKI Registration Authority shall confirm by email, to the SRO as identified on the Authorised Subscriber / Interface Access Application Form, that the applicant organisation has become an Authorised Subscriber for Device Certificates and will also notify the Service Desk.	SMKI Registration Authority	5.5.16

5.5.16	As soon as reasonably practicable, following 5.5.15	The SMKI Registration Authority shall arrange and conduct a meeting, as soon as reasonably practicable, at which the credentials as set out in steps 5.4.2, 5.4.3 and 5.4.5 (as set out in Section 5.4 of this document) shall be provided, as appropriate.	SMKI Registration Authority	5.5.17
5.5.17	As soon as reasonably practicable, following 5.5.11 or 5.5.16	Update the DCC's list of Authorised Subscribers for Organisation Certificates and/or Device Certificates, for audit purposes.	SMKI Registration Authority	End of procedure

6. SMKI Registration Authority registration procedures

The procedures as set out in SMKI RAPP Sections 6.2 to 6.4 shall be undertaken in order for nominated individuals to act on behalf of the SMKI Registration Authority as a SMKI Registration Authority Manager or a member of SMKI Registration Authority Personnel.

6.1 General registration obligations

The SMKI Registration Authority shall:

a) not permit any nominated individual to access Systems used to provide SMKI Services and/or the SMKI Repository Service as a SMKI Registration Authority Manager or member of SMKI Registration Authority Personnel until the procedures in SMKI RAPP Sections 6.2 or 6.3 have been successfully completed;

b) in performing the procedures as set out in SMKI RAPP Sections 6.2 and 6.3, store and maintain records relating to individuals becoming SMKI Registration Authority Managers and SMKI Registration Authority Personnel, in accordance with the Code and the DCC's data retention policy;

c) ensure that, at all times, there are at least two SMKI Registration Authority Managers;

d) if there is a material change to any of the information used to verify the identity of any SMKI Registration Authority Manager or member of SMKI Registration Authority Personnel, ensure that its SMKI Registration Authority Manager or member of SMKI Registration Authority Personnel undertakes the procedures as set out in SMKI RAPP Sections 6.2 or 6.3 in respect of the revised evidence of identity; and

e) check the name and address of the SMKI Registration Authority Manager or member of the SMKI Registration Authority Personnel before issuing a replacement token.

The DCC shall ensure that:

a) for authentication credentials issued under the IKI Certificate Policy to Authorised Responsible Officers, such authentication credentials have a lifetime of ten years following issuance of such authentication credentials and shall cease to function upon after ten years following issuance; and

b) for authentication credentials not issued under the IKI Certificate Policy, that such authentication credentials remain valid until revoked.

6.2 Procedure for becoming a SMKI Registration Authority Manager

The procedure for becoming a SMKI Registration Authority Manager as detailed immediately below shall be conducted by DCC's Chief Information Security Officer (CISO), or an individual that they have authorised to act on their behalf in this capacity, on behalf of the DCC, in order to nominate, authorise and verify a SMKI Registration Authority Manager.

Step	When	Obligation	Responsibility	Next Step
6.2.1	As required	Nominate an individual to become a SMKI Registration Authority Manager, who shall be an employee of the DCC or be contracted to the DCC, and advise the nominated individual of the evidence to be provided in order to verify their identity.	DCC Chief Information Security Officer, on behalf of the DCC	6.2.2
6.2.2	As soon as reasonably practicable following 6.2.1	Confirm verification meeting date/time with nominated individual.	DCC Chief Information Security Officer, on behalf of the DCC	6.2.3
6.2.3	In verification meeting	The CISO shall, in accordance with the provisions of Sections G4.4 to G4.8: a. check proof of identity provided against the information provided by the nominated individual; and b. verify the identity of the nominated individual to the level pursuant to the SMKI PMA Guidance on "Verifying Individual Identity" published on the Website.	DCC Chief Information Security Officer, on behalf of the DCC	If verified, 6.2.5. If not verified, 6.2.4
6.2.4	In verification meeting	If the identity of the nominated individual is not successfully verified, provide reasons for the failure to the individual and notify the individual that a further verification meeting is required to remedy the unsuccessful elements of the verification.	DCC Chief Information Security Officer, on behalf of the DCC	6.2.5
6.2.5	In verification meeting	If the identity of the nominated individual is successfully verified, notify the individual verbally and subsequently in writing that they have become a SMKI Registration Authority Manager and notify the SMKI PMA that the	DCC Chief Information Security Officer, on behalf of the DCC	6.2.6

		nominated individual has become a SMKI Registration Authority Manager.		
6.2.6	As soon as reasonably practicable following 6.2.5	Record the details of the individual that has become a SMKI Registration Authority Manager, in a manner which is auditable.	SMKI Registration Authority	Procedure as set out in SMKI RAPP Section 6.4

6.3 Procedure for becoming a member of SMKI Registration Authority Personnel

The procedure for becoming a member of SMKI Registration Authority Personnel as detailed immediately below shall be conducted by a SMKI Registration Authority Manager on behalf of the SMKI Registration Authority, in order to nominate, verify, authorise and provide means for authenticating access to Systems used to provide SMKI Services and/or the SMKI Repository Service in respect of a member of SMKI Registration Authority Personnel.

Step	When	Obligation	Responsibility	Next Step
6.3.1	As required	Nominate an individual to become a member of SMKI Registration Authority Personnel, who shall be an employee of the DCC or be contracted to the DCC.	SMKI Registration Authority Manager, on behalf of the SMKI Registration Authority	6.3.2
6.3.2	As soon as reasonably practicable following 6.3.1	Confirm verification meeting date/time with nominated individual.	SMKI Registration Authority Manager, on behalf of the SMKI Registration Authority	6.3.3
6.3.3	In verification meeting	In the verification meeting, the SMKI Registration Authority Manager shall, in accordance with the provisions of Sections G4.4 to G4.8: a. check proof of identity provided against the information provided by the nominated individual; and b. verify the identity of the nominated individual to the level pursuant to the SMKI PMA Guidance on "Verifying Individual Identity" published on the Website.	SMKI Registration Authority Manager, on behalf of the SMKI Registration Authority	If successful, 6.3.5. If not successful, 6.3.4
6.3.4	In verification meeting	If the identity of the nominated individual is not successfully verified, provide reasons for the rejection to the individual and notify the	SMKI Registration Authority Manager, on behalf of the	6.3.2

		individual that a further meeting is required to remedy the affected elements of the verification.	SMKI Registration Authority	
6.3.5	As soon as reasonably practicable, following 6.3.3	If the identity of the nominated individual is successfully verified, notify the individual verbally and subsequently in writing that they have become a member of SMKI Registration Authority Personnel.	SMKI Registration Authority Manager, on behalf of the SMKI Registration Authority	6.3.6
6.3.6	As soon as reasonably practicable following 6.3.5	Record the details of the individual that has become a member of SMKI Registration Authority Personnel in respect of the SMKI Registration Authority, in a manner which is auditable.	SMKI Registration Authority	Procedure as set out in SMKI RAPP Section 6.4

6.4 Procedure for provision of credentials to a SMKI Registration Authority Manager or a member of SMKI Registration Authority Personnel

The procedure for provision of credentials to a SMKI Registration Authority Manager or a member of SMKI Registration Authority Personnel, as detailed immediately below, shall be conducted by the DCC's CISO in respect of a SMKI Registration Authority Manager or a SMKI Registration Authority Manager in respect of a member of SMKI Registration Authority Personnel.

Step	When	Obligation	Responsibility	Next Step
6.4.1	In verification meeting, following confirmation of becoming a SMKI Registration Authority Manager or member of SMKI Registration Authority Personnel	Provide credentials in accordance with step 6.4.2 or 6.4.3 below, depending on whether the individual has become a SMKI Registration Authority Manager or a member of SMKI Registration Authority Personnel.	DCC CISO or SMKI Registration Authority Manager	If providing to a SMKI Registration Authority Manager, 6.4.2; if providing to a member of SMKI Registration Authority Personnel, 6.4.3
6.4.2	In verification meeting, following confirmation	Provide the SMKI Registration Authority Manager with credentials as listed immediately below, to be used to perform activities on behalf of the SMKI Registration Authority: a. one Cryptographic Credential Token	DCC CISO	6.4.4

	of becoming a SMKI Registration Authority Manager	containing authentication credentials issued under the IKI Certificate Policy which can be used to authenticate the individual to the SMKI Portal; and b. usernames and passwords enabling for the purposes of authentication to the SMKI Repository portal.		
6.4.3	In verification meeting, following confirmation of becoming a member of SMKI Registration Authority Personnel	Provide the member of SMKI Registration Authority Personnel with credentials as listed immediately below, to be used to perform activities on behalf of the SMKI Registration Authority: a. one Cryptographic Credential Token containing authentication credentials issued under the IKI Certificate Policy which can be used to authenticate the individual to the SMKI Portal; and b. usernames and passwords enabling for the purposes of authentication to the SMKI Repository Portal.	SMKI Registration Authority Manager	6.4.4
6.4.4	In verification meeting, following issuance of credentials	The SMKI Registration Authority Manager or member of SMKI Registration Authority Personnel shall sign that they accept the credentials issued to them on the Cryptographic Credential Token. Where the SMKI Registration Authority Manager or member of SMKI Registration Authority Personnel does not accept the credentials they shall notify the DCC's CISO (in the case of the SMKI Registration Authority Manager) or otherwise the SMKI Registration Authority Manager and shall not sign for the Cryptographic Credential Token.	SMKI Registration Authority Manager or member of SMKI Registration Authority Personnel	End of Procedure

7. Submission of CSRs and Issuance of Certificates

7.1 Submission of Certificate Signing Requests

The SMKI Interface Design Specification (SMKI IDS) and the Code sets out the provisions in respect of:

a) the mechanism established for this purpose is in accordance with the procedure in PKCS#10;

b) naming restrictions in respect of the Subject of each Certificate in accordance with the relevant Certificate Policy;

c) the circumstances in which an Authorised Subscriber may submit a Certificate Signing Request (CSR) in respect of a Device Certificate and the means by which it may do so (SMKI IDS sections 2.3.1.6, 2.4.1.1 and 2.5.1.1);

d) the circumstances in which an Authorised Subscriber may submit a CSR in respect of an Organisation Certificate and the means by which it may do so (SMKI IDS sections 2.3.1.1 and 2.6.1.1);

e) the circumstances in which an Authorised Subscriber for an IKI Certificate may submit a CSR in respect of an IKI Certificate and the means by which it may do so (SMKI IDS sections 2.4 and 2.5); and

f) requirements in respect of validation of the format of a CSR, checking that the submitting organisation is an Eligible Subscriber for the Certificate and rejection if such requirements are not met.

The SMKI Registration Authority shall validate the Subject of each CSR in respect of an Organisation Certificate to ensure that each CSR corresponds with an EUI-64 Compliant identifier range that is applicable to the relevant User Role, as provided in the Organisation Information Form.

Subject to the provisions of the Code and this SMKI RAPP, the DCC shall accept requests for copies of Organisation Certificates and/or Device Certificates from non DCC Users by phone via the Service Desk or, in the case of Organisation Certificates, via the SMKI Portal via the Internet. The DCC shall, following such a request, provide the relevant information as soon as is reasonably practicable, via a secured electronic means.

7.2 Processing of CSRs for XML Signing Certificates

Upon receipt of a Certificate Signing Request from a Supplier Party seeking to be Issued with an Organisation Certificate that has a Remote Party Role of xmlSign and where that Supplier Party is seeking to include within the Subject X520 Common Name field (with the meaning given to that term in the Organisation Certificate Policy) one or more Market Participant Identifier(s) by which that Supplier Party may be identified in the Party Details, the SMKI Registration Authority shall reject that Certificate Signing Request if:

a) there is more than one such identifier that relates to the supply of gas;

b) there is more than one such identifier that relates to the supply of electricity;

c) the Market Participant Identifier(s) included with the Certificate Signing Request are identifiers that the Panel has notified the DCC are not associated with that Supplier Party pursuant to Section B1.21 of the Code; and

d) any of the Market Participant Identifier(s) included within the Certificate Signing Request is already included within the Subject X520 Common Name field (with the meaning given to that term in the Organisation Certificate Policy) of another Organisation Certificate that has been Issued to a different Supplier Party and any such other Organisation Certificate:

   i. has not been revoked; or

   ii. has not expired.

7.3 Issuance of Certificates

The SMKI Interface Design Specification sets out the provisions in respect of:

a) the circumstances in which the DCA shall issue Device Certificates (SMKI IDS sections 2.3.1.9, 2.4.1.4 and 2.5.1.4);

b) the circumstances in which the OCA shall issue Organisation Certificates (SMKI IDS sections 2.3.1.4 and 2.6.1.4);

c) the circumstances in which the ICA shall issue IKI Certificates (SMKI IDS sections 2.4 and 2.5); and

d) the obligations in respect of lodging Certificates in the SMKI Repository (SMKI IDS sections 2.3.1.4, 2.3.1.9, 2.4.1.4 and 2.5.1.4).

8. Revocation

The procedures as set out in this Section 8 shall be undertaken for the revocation of Certificates except where SEC Section L16 (Supplier of Last Resort) applies.

8.1 Revocation of Device Certificates

In line with the Device Certificate Policy section 4.9.1, Device Certificates cannot be revoked.

8.2 Revocation of Organisation Certificates

8.2.1 General Organisation Certificate revocation obligations

The DCC shall permit each of the following individuals to request the revocation of an Organisation Certificate, where the reasons for such revocation request must be one of the permitted reasons for Organisation Certificate revocation as set out in Section 4.9.1 in Appendix B of the Code:

a) Any SMKI PMA member, on behalf of the SMKI PMA;

b) Any Senior Responsible Officer for a Subscriber for an Organisation Certificate; or

c) Any SMKI Registration Authority Manager or member of SMKI Registration Authority Personnel, on behalf of the DCC.

The DCC, in its role as SMKI Registration Authority, shall only accept CRRs through the following mechanisms (or a combination of such mechanisms):

a) in writing, via registered post;

b) via a secured electronic means; or

c) in person, at the offices of the SMKI Registration Authority, where the address of such offices shall be as set out on the DCC Website.

The revocation of an Organisation Certificate shall be permanent and the SMKI Registration Authority shall ensure that no revoked Organisation Certificate may be reinstated.

The DCC shall, each month, prepare and submit a report to the SMKI PMA regarding the number and nature of Organisation Certificate revocations. A null report is not required.

8.2.2 Procedure for Organisation Certificate Revocation

The procedure for authorisation, verification and, where verified, revocation of Certificates is as set out immediately below.

Step	When	Obligation	Responsibilit y	Next Step
8.2.2.1	As soon as reasonably practicable when Certificate revocation is required	A SMKI PMA Member on behalf of the SMKI PMA, an SRO on behalf of a Subscriber or the SMKI Registration Authority Manager or a member of SMKI Registration Authority Personnel on behalf of the DCC shall submit, using the mechanisms set out in SMKI RAPP Section 8.2.1, a CRR to the SMKI Registration Authority. The reason for such CRR shall be one of the permitted reasons for Organisation Certificate revocation as set out in Section 4.9 in Appendix B of the Code. Each CRR shall contain the following information, as set out in SMKI RAPP Annex A (A7) : a. Identify the Subscriber; b. Identify the individual who is submitting the CRR; c. Unambiguously (i.e. by specifying the serial number of the Certificate) identify the Certificate to be revoked; and d. State the reason for the Certificate revocation.	SMKI PMA Member, Subscriber requiring Organisation Certificate revocation or SMKI Registration Authority Manager or SMKI Registration Authority Personnel	8.2.2.2
8.2.2.2	As soon as reasonably practicable, following 8.2.2.1	On receipt of a CRR, notify the SMKI Registration Authority Manager for verification, processing and/or approval. The SMKI Registration Authority shall treat each CRR and any associated circumstances as confidential. Where the CRR is submitted by an SMKI Registration Authority Manager, the approval in this step must be sought from a different SMKI Registration Authority Manager or the DCC’s CISO.	SMKI Registration Authority Personnel	8.2.2.3
8.2.2.3	As soon as reasonably practicable following receipt	Where it has been submitted by an SRO, validate the Certificate Revocation Request by contacting a Senior Responsible Officer and confirming details for the SRO as provided in the original application to become an SRO: a. Where submitted in writing, the SMKI Registration Authority shall send an email	SMKI Registration Authority Manager or DCC's CISO	If validated, 8.2.2.5; if invalid (considere d malicious

		to a Senior Responsible Officer. The SMKI Registration Authority shall 1) confirm such information from the relevant SRO Nomination Form, in order to provide confidence that the request is from an authorised SRO; 2) confirm the details of the Organisation Certificate to which the revocation request received relates (as provided in the submitted letter); and 3) confirm that a reason for the request has been specified in accordance with section 4.9.2 of the Organisation Certificate Policy. b. Where submitted in person, the SMKI Registration Authority shall 1) verify the handwritten signature of the Senior Responsible Officer against that held by the SMKI Registration Authority; 2) confirm details provided in the relevant SRO Nomination Form, in order determine that the request is authentic; 3) confirm the details of the Organisation Certificate to which the CRR received relates; and 4) confirm that a reason for the request has been specified in accordance with section 4.9.2 of the Organisation Certificate Policy. Where the Certificate Revocation Request was submitted by a SMKI Registration Authority Manager, a member of the SMKI Registration Authority Personnel or a member of the SMKI PMA, validate the Certificate Revocation Request by contacting a SMKI Registration Authority Manager or the SMKI PMA to confirm details of the Certificate Revocation Request.		and/or inauthentic) or incomplete , 8.2.2.4

8.2.2.4	As soon as reasonably practicable following unsuccessful validation	Where the Certificate Revocation Request is not validated as in 8.2.2.3, reject the revocation request and notify the individual that was contacted in step 8.2.2.3 to validate the revocation request, in writing, including the reasons for rejection and identify resulting steps to be taken.	SMKI Registration Authority Manager or DCC's CISO	End of procedure

8.2.2.5	As soon as reasonably practicable following successful validation	Where the Certificate Revocation Request is validated in 8.2.2.3, the DCC shall carry out a check that the	SMKI Registration Authority Manager (s) and/or DCC's CISO (as needed for two party approval).	8.2.2.6

		correct Certificate is to be revoked and to obtain and record two-party approval of the authorisation and record the time from which the revocation is to take effect.		
8.2.2.6	As soon as reasonably practicable following 8.2.2.5	Revoke the identified Organisation Certificate that is the subject of the CRR.	SMKI Registration Authority Manager	8.2.2.7
8.2.2.7	As soon as reasonably practicable following notification, or every hour (whichever is sooner)	Update the relevant Certificate Revocation List (CRL) and publish such CRL to the SMKI Repository, as set out in Appendix B of the Code, section 4.9.7 (D).	SMKI Registration Authority	8.2.2.8
8.2.2.8	Following revocation	Notify the individual submitting the CRR of the successful revocation of the Organisation Certificate in the CRR, by email.	SMKI Registration Authority Manager	End of procedure

8.3 Revocation of SMKI Services and / or the SMKI Repository Service access credentials and / or IKI File Signing Certificates

8.3.1 General obligations relating to revocation of ARO credentials for accessing SMKI Services and / or the SMKI Repository Service and / or File Signing Certificates

A Senior Responsible Officer on behalf of a Party, RDP, Manufacturer, SECCo or the DCC (in its role as DCC Service Provider) may request the revocation of access credentials in respect of an Authorised Responsible Officer acting on behalf of that Party, RDP, Manufacturer, SECCo or the DCC (as DCC Service Provider) or revocation of an IKI File Signing Certificate for which that Party, RDP, Manufacturer, SECCo is an Authorised Subscriber, using the form as set out in Annex A (A7) and clearly identifying the credentials to be revoked.

The permitted reasons for revocation of authentication credentials shall be as listed immediately below:

a) An applicant wishes an IKI File Signing Certificate or the credentials of an ARO to be revoked.

b) A Party, RDP, Manufacturer, SECCo or the DCC (as DCC Service Provider), of which the ARO is a representative, becomes ineligible to access SMKI Services and/or the SMKI Repository Service or ceases to become an Authorised Subscriber for Device Certificates or Organisation Certificates, or both, as appropriate.

c) If there is a change to any of the information that was used to verify the identity of an ARO (but where the renewal or replacement of documents used to verify such identity, where the identity information remains the same, shall not constitute a change).

d) A Party, RDP, Manufacturer, DCC (as DCC Service Provider), or SECCo notifies the SMKI Registration Authority that it reasonably believes that the ARO is a threat to the security, integrity, or stability of the SMKI Services and/or the SMKI Repository Service.

e) The information on which the identity of an ARO was established is known, or is reasonably suspected, to be inaccurate.

f) The authentication credentials issued to the ARO are lost, stolen, inoperative, or destroyed. The DCC shall ensure that the Cryptographic Credential Token issued to an ARO is automatically rendered inoperative where the PIN code on the Cryptographic Credential Token used to access SMKI Services has been entered incorrectly 15 consecutive times.

Where access credentials have been revoked and the Party, RDP, Manufacturer, SECCo or DCC (as DCC Service Provider) wishes to receive new access credentials, that Party, RDP, Manufacturer, SECCo or DCC (as DCC Service Provider) shall submit a new ARO Nomination Form.

8.3.2 Procedure for revocation of SMKI Services and / or the SMKI Repository Service access credentials for AROs and / or IKI File Signing Certificates

The procedure for verification and, where verified, revocation of authentication credentials or IKI File Signing Certificates is as set out immediately below.

Step	When	Obligation	Responsibility	Next Step
8.3.2.1	As required	Complete the Credential Revocation Request Form as set out in SMKI RAPP Annex A (A7), ensuring that the information entered on the form is complete and accurate, and the Credential Revocation Request Form is authorised by an SRO on behalf of the applicant organisation.	SRO on behalf of the applicant organisation, which shall be a Party, RDP, Manufacturer, SECCo or DCC (as DCC Service Provider)	8.3.2.2

8.3.2.2	As required, following 8.3.2.1	Submit the completed Credential Revocation Request Form to the SMKI Registration Authority via a secured electronic means, as directed on the DCC Website.	SRO on behalf of the applicant organisation, which shall be a Party, RDP, Manufacturer, SECCo or DCC (as DCC Service Provider)	8.3.2.3
8.3.2.3	As soon as reasonably practicable following 8.3.2.2	Acknowledge receipt by email to the SRO as identified on the Credential Revocation Request Form or via the Service Desk updating the relevant ticket, ensuring a record is kept.	SMKI Registration Authority or Service Desk	8.3.2.4
8.3.2.4	As soon as reasonably practicable following 8.3.2.3	Analyse the information entered on the Credential Revocation Request Form; determine completeness and any discrepancies. Where there are omissions/discrepancies, agree actions with an SRO via email.	SMKI Registration Authority	If complete, 8.3.2.6; if not complete, 8.3.2.5
8.3.2.5	Once omissions / discrepancies are addressed	Submit a revised Credential Revocation Request Form to the SMKI Registration Authority via a secured electronic means, as directed on the DCC Website.	SRO on behalf of the applicant organisation, which shall be a Party, RDP, Manufacturer, SECCo or DCC (as DCC Service Provider)	8.3.2.3
8.3.2.6	As soon as reasonably practicable, following 8.3.2.4	Contact the SRO as identified on the Credential Revocation Request Form, using the registered contact information for the SRO as held by the SMKI Registration Authority, to confirm the application identified by the Credential Revocation Request Form is authorised.	SMKI Registration Authority	If confirmed as authorised, 8.3.2.8; if not authorised, 8.3.2.7
8.3.2.7	As soon as reasonably practicable following rejection	Notify the SRO that was contacted in step 8.3.2.3, that the procedure in respect of the application has not been successful, by email.	SMKI Registration Authority	End of procedure

8.3.2.8	As soon as reasonably practicable following 8.3.2.6	Notify the SRO that was contacted in step 8.3.2.3, and the DCC's CISO by email that the revocation request has been accepted.	SMKI Registration Authority Personnel, on behalf of the SMKI Registration Authority	8.3.2.9

8.3.2.9	As soon as reasonably practicable following 8.3.2.8	Revoke the credentials for the relevant service, for the identified ARO or relevant IKI File Signing Certificate as indicated by the SRO on the Credential Revocation Request Form. In doing so, the DCC shall, where required to revoke the credentials, revoke all associated IKI Certificates. DCC shall ensure that access to the relevant service is prevented from the point of revocation.	SMKI Registration Authority Personnel, on behalf of the SMKI Registration Authority	8.3.2.10

8.3.2.10	As soon as reasonably practicable following 8.3.2.9	Notify the SRO that was contacted in step 8.3.2.3 of the successful revocation of credentials for the ARO or relevant IKI File Signing Certificate. Where such revocation results in the individual that is the subject of the Credential Revocation Request Form no longer having any valid credentials issued to them in accordance with the SMKI RAPP, the SMKI Registration Authority shall notify the SRO that was contacted in step 8.3.2.3 that the individual is no longer an ARO, by email.	SMKI Registration Authority Personnel, on behalf of the SMKI Registration Authority	8.3.2.11

8.3.2.11	As soon as reasonably practicable following 8.3.2.10	Where the revoked credentials were issued on a Cryptographic Credential Token or Cryptographic Credential Tokens, the Party, RDP, Manufacturer, SECCo or DCC Service Provider shall, where such Cryptographic Credential Tokens are in the possession of the applicant organisation, send the Cryptographic Credential Token or Cryptographic	SRO on behalf of the applicant organisation	8.3.2.12

		Credential Tokens to the DCC, via secure courier.		

8.3.2.12	As soon as reasonably practicable following 8.3.2.11	The DCC shall verifiably destroy all Secret Key Material or Certificates contained on the returned Cryptographic Credential Token.	SMKI Registration Authority Manager, on behalf of the SMKI Registration Authority	8.3.2.13

8.3.2.13	As soon as reasonably practicable following 8.3.2.12	Record the details of the credentials that have been revoked in respect of the ARO as identified on the Credential Revocation Request Form or relevant IKI File Signing Certificate, plus, if relevant, update the DCC's list of AROs, in a manner which is auditable.	SMKI Registration Authority	End of procedure

8.3.3 General obligations relating to revocation of SMKI Registration Authority Manager or SMKI Registration Authority Personnel credentials for accessing SMKI Services and / or the SMKI Repository Service

The following parties may request the revocation of authentication credentials in respect of SMKI Registration Authority Personnel, using the form referred to in Annex A (A7):

a) Any SMKI PMA member, on behalf of the SMKI PMA;

b) A SMKI Registration Authority Manager, on behalf of the SMKI Registration Authority; and

c) DCC's CISO.

The permitted reasons for revocation of authentication credentials shall be as listed immediately below:

a) A SMKI Registration Authority Manager or DCC's CISO wishes the credentials of a SMKI Registration Authority Manager or member of SMKI Registration Authority Personnel to be revoked.

b) A member of SMKI Registration Authority Personnel becomes ineligible to access SMKI Services and/or the SMKI Repository Service.

c) A member of SMKI Registration Authority Personnel fails to comply with Appendix A, Appendix B and Appendix Q of the Code, or this SMKI RAPP.

d) Any information used to verify the identity of a member of SMKI Registration Authority Personnel changes, the individual leaves the employment of the DCC, or moves within DCC to a role in which they are not entitled to access SMKI Services and/or the SMKI Repository Service.

e) A SMKI Registration Authority Manager becomes aware that the member of SMKI Registration Authority Personnel or a SMKI Registration Authority Manager is a potential threat to the security, integrity, or stability of the SMKI Services and/or the SMKI Repository Service.

f) The information on which the identity of a SMKI Registration Authority Manager or member of SMKI Registration Authority Personnel was established is known, or is suspected, to be inaccurate.

g) The authentication credentials issued to a member of SMKI Registration Authority Personnel are lost, stolen, inoperative, or destroyed. The DCC shall ensure that the Cryptographic Credential Token issued to a member of SMKI Registration Authority Personnel is automatically rendered inoperative where the PIN code on the Cryptographic Credential Token used to access SMKI Services has been entered incorrectly 15 consecutive times.

8.3.4 Procedure for revocation of SMKI Services access credentials for SMKI Registration Authority Managers and SMKI Registration Authority Personnel

The procedure for verification and, where verified, revocation of credentials in respect of a SMKI Registration Authority Manager or member of SMKI Registration Authority Personnel is as set out immediately below.

Step	When	Obligation	Responsibility	Next Step
8.3.4.1	As required	Complete the Credential Revocation Request Form as set out in SMKI RAPP Annex A (A7), ensuring that the information entered on the form is complete and accurate, and the Credential Revocation Request Form is authorised: a. for a member of SMKI Registration Authority Personnel, by a SMKI Registration Authority Manager; or b. for a SMKI Registration Authority Manager, by the DCC's CISO.	DCC CISO, SMKI Registration Authority Manager, or SMKI PMA Member	8.3.4.2
8.3.4.2	As required, following 8.3.4.1	Submit the completed Credential Revocation Request Form to a SMKI Registration Authority Manager.	DCC CISO, SMKI Registration Authority Manager, or SMKI PMA Member	8.3.4.3
8.3.4.3	As soon as reasonably practicable following 8.3.4.2	Analyse the information entered on the Credential Revocation Request Form; determine completeness and any discrepancies. Where there are omissions/discrepancies, agree amendments and adjust form contents.	SMKI Registration Authority Manager, on behalf of the SMKI Registration Authority	8.3.4.4

8.3.4.4	As soon as reasonably practicable following 8.3.4.3	Revoke the credentials of the identified SMKI Registration Authority Manager or member of SMKI Registration Authority Personnel as indicated on the Credential Revocation Request Form. Where the Credential Revocation Request is validated as in 8.3.4.3, the DCC shall carry out a check that the correct credential is to be revoked and record approval of the authorisation.	SMKI Registration Authority Manager, on behalf of the SMKI Registration Authority	8.3.4.5
8.3.4.5	As soon as reasonably practicable following 8.3.4.4	Where such revoked credentials were issued on a Cryptographic Credential Token, the DCC shall retrieve such Cryptographic Credential Token from the identified SMKI Registration Authority Manager or member of SMKI Registration Authority Personnel and shall verifiably destroy all Secret Key Material or Certificates contained on the Cryptographic Credential Token.	SMKI Registration Authority Manager, on behalf of the SMKI Registration Authority	8.3.4.6
8.3.4.6	As soon as reasonably practicable following 8.3.4.5	Record the details of the credentials that have been revoked in respect of the member of SMKI Registration Authority Personnel or SMKI Registration Authority Manager as identified on the Credential Revocation Request Form.	SMKI Registration Authority Manager, on behalf of the SMKI Registration Authority	8.3.4.7
8.3.4.7	As soon as reasonably practicable following 8.3.4.5	Notify DCC's CISO or SMKI Registration Authority Manager who submitted the original Credential Revocation Request Form that the revocation has been completed.	SMKI Registration Authority Manager, on behalf of the SMKI Registration Authority	End of procedure

Annex A – Form Templates

The form templates listed in Annex A are available from the DCC Website or via the DCC SharePoint site as advised by the DCC.

The DCC may, subject to the approval of the SMKI PMA, modify the form templates from time to time.

A1. **Organisation Information Form**

A2. **Authorised Subscriber / Interface Access Application Form**

A3. **SMKI SRO Nomination Form**

A4. **SMKI ARO Nomination Form**

A5. **Nominee Details Form**

A6. **Organisation Certificate Revocation Request Form**

A7. **Credential Revocation Request Form**

Annex B – Definitions

In this Policy, except where the context otherwise requires:

- expressions defined in Section A of the Code (Definitions and Interpretation) have the same meaning as is set out in that Section;
- the expressions in the left hand column below shall have the meanings given to them in the right hand column below; and
- where any expression is defined in Section A of the Code (Definitions and Interpretation) and in this Annex, the definition in this Annex shall take precedence for the purposes of this document.

Ad Hoc Device CSR Web Service	The system-to-system interface provided for the purposes of Authorised Subscribers systems submitting individual CSRs in respect of Device Certificates.
Authorised Responsible Officer (ARO)	Means an individual that has successfully completed the process for becoming an ARO on behalf of a Party, RDP, Manufacturer, SECCo or a DCC Service Provider in accordance with the SMKI RAPP and/or the DCCKI RAPP (as applicable).
Authorised Subscriber / Interface Access Application Form	Means the for as specified in section A2 of this SMKI RAPP.
Batched Device CSR Web Service	The system-to-system interface provided for the purposes of Authorised Subscribers systems submitting batches of CSRs in respect of Device Certificates and subsequently a synchronous mechanism to retrieve the resulting Device Certificates.
Chief Information Security Officer (CISO)	Has the meaning given to that expression in the SMKI Recovery Procedure.
Certificate Revocation Request	Has the meaning given to that expression in the Organisation Certificate Policy.

Credential Revocation Request Form	Means the form as specified in section A7 of this SMKI RAPP.
Cryptographic Credential Token	Means a FIPS 140-2 Level 3 token containing Secret Key Material, as issued in accordance with the SMKI RAPP
IKI Certification Authority	Has the meaning given to that expression in the IKI Certificate Policy.
Issue	Has the meaning given to that expression in SEC Section A and like terms shall be interpreted accordingly.
Nominee Details Form	Means the form as specified in section A5 of this SMKI RAPP.
Organisation Certificate Revocation Request Form	Means the form as specified in section A6 of this SMKI RAPP.
Organisation Information Form	Means the form as specified in section A1 of this SMKI RAPP.
Party	Has the meaning set out in SEC Section A except for the DCC, which shall not be a Party in this document.
SMKI Portal	Has the meaning given to that expression in the SMKI Interface Design Specification.
SMKI Registration Authority	Means the DCC acting in its capacity as such for the purposes of the Organisation Certificate Policy, Device Certificate Policy or IKI Certificate Policy.
SMKI Registration Authority Manager	Means an individual who acts on behalf of the SMKI Registration Authority to perform tasks relating to the management of the SMKI Registration Authority, as set out in the SMKI RAPP
SMKI Registration Authority Personnel	Means those persons who are engaged by DCC, in so far as such persons carry out functions of the SMKI Registration Authority as set out in the SMKI RAPP
SMKI ARO Nomination Form	Means the form as specified in section A4 of this SMKI RAPP.
SMKI SRO Nomination Form	Means the form as specified in section A3 of this SMKI RAPP.

Senior Responsible Officer (SRO)	Means an individual that has successfully completed the process for becoming an SRO on behalf of a Party, RDP, Manufacturer, SECCo or a DCC Service Provider in accordance with the SMKI RAPP and/or the DCCKI RAPP (as applicable).

Version E 8.0

APPENDIX E

DCC User Interface Services Schedule

Contents

DCC USER INTERFACE SERVICES SCHEDULE

Service Reference	Service Reference Variant	Description	Eligible Users	SMETS2+ Target Response Time	SMETS1 Target Response Time	Non-Device Services	Notes
1.1	1.1.1	Update Import Tariff (Primary Element)	Import Supplier, Gas Supplier	30 seconds	16 seconds		
1.1	1.1.2	Update Import Tariff (Secondary Element)	Import Supplier	30 seconds	n/a		Users may only be Eligible Users for this Service in respect of SMETS2+ Devices
1.2	1.2.1	Update Price (Primary Element)	Import Supplier, Gas Supplier	24 hours	24 hours		
1.2	1.2.2	Update Price (Secondary Element)	Import Supplier	24 hours	n/a		Users may only be Eligible Users for this Service in respect of SMETS2+ Devices
1.5	1.5	Update Meter Balance	Import Supplier, Gas Supplier	30 seconds	16 seconds		
1.6	1.6	Update Payment Mode	Import Supplier, Gas Supplier	30 seconds	16 seconds		
1.7	1.7	Reset Tariff Block	Import Supplier	30 seconds	n/a		Users may only be Eligible Users for

		Counter Matrix					this Service in respect of SMETS2+ Devices
2.1	2.1	Update Prepay Configuration	Import Supplier, Gas Supplier	30 seconds	16 seconds		
2.2	2.2	Top Up Device	Import Supplier, Gas Supplier	30 seconds	16 seconds		
2.3	2.3	Update Debt	Import Supplier, Gas Supplier	30 seconds	16 seconds		
2.5	2.5	Activate Emergency Credit	Import Supplier, Gas Supplier	30 seconds	16 seconds		
3.1	3.1	Display Message	Import Supplier, Gas Supplier	30 seconds	n/a		Users may only be Eligible Users for this Service in respect of SMETS2+ Devices
3.2	3.2	Restrict Access for Change of Tenancy	Import Supplier, Gas Supplier	30 seconds	16 seconds		
3.3	3.3	Clear Event Log	Import Supplier, Gas Supplier	30 seconds	16 seconds		
3.4	3.4	Update Supplier Name	Import Supplier, Gas Supplier	24 hours	n/a		Users may only be Eligible Users for this Service in respect of SMETS2+ Devices

3.5	3.5	Disable Privacy PIN	Import Supplier, Gas Supplier	30 seconds	n/a		Users may only be Eligible Users for this Service in respect of SMETS2+ Devices
4.1	4.1.1	Read Instantaneous Import Registers	Import Supplier, Gas Supplier, Electricity Distributor, Gas Transporter	30 seconds	16 seconds		
4.1	4.1.2	Read Instantaneous Import ToU Matrices	Import Supplier, Gas Supplier, Electricity Distributor, Gas Transporter	30 seconds	16 seconds		
4.1	4.1.3	Read Instantaneous Import ToU with Blocks Matrices	Import Supplier, Electricity Distributor	30 seconds	16 seconds		
4.1	4.1.4	Read Instantaneous Import Block Counters	Gas Supplier	30 Seconds	16 seconds		
4.2	4.2	Read Instantaneous Export Register Values	Export Supplier, Electricity Distributor	30 seconds	16 seconds		
4.3	4.3	Read Instantaneous Prepayment	Import Supplier, Gas Supplier	30 seconds	16 seconds		

		Register Values					
4.4	4.4.2	Retrieve Change of Mode / Tariff Triggered Billing Data Log	Import Supplier, Gas Supplier,	30 seconds	16 seconds		
4.4	4.4.3	Retrieve Billing Calendar Triggered Billing Data Log	Import Supplier, Gas Supplier	30 seconds	16 seconds		
4.4	4.4.4	Retrieve Billing Data Log (Payment Based Debt Payments)	Import Supplier, Gas Supplier	30 seconds	16 seconds		
4.4	4.4.5	Retrieve Billing Data Log (Prepayment Credits)	Import Supplier, Gas Supplier	30 seconds	16 seconds		
4.6	4.6.1	Retrieve Import Daily Read Log	Import Supplier, Gas Supplier	30 seconds	16 seconds		Where a change of supplier occurs on any day, both the new supplier and the old supplier will be eligible to retrieve the daily read log for that day.
4.6	4.6.2	Retrieve Export Daily Read Log	Export Supplier	30 seconds	n/a		Where a change of supplier occurs on any day, both the new supplier and the old supplier will be eligible to retrieve the daily

							read log for that day. Users may only be Eligible Users for this Service in respect of SMETS2+ Devices

4.8	4.8.1	Read Active Import Profile Data	Import Supplier, Gas Supplier, Electricity Distributor, Gas Transporter, Other User	5,600 seconds	16 seconds		

4.8	4.8.2	Read Reactive Import Profile Data	Import Supplier, Electricity Distributor, Other User	30 seconds	16 seconds		

4.8	4.8.3	Read Export Profile Data	Export Supplier, Electricity Distributor, Other User	30 seconds	16 seconds		

4.10	4.10	Read Network Data	Import Supplier, Gas Supplier, Electricity Distributor, Gas Transporter	30 seconds	16 seconds		

4.11	4.11.1	Read Tariff (Primary Element)	Import Supplier, Gas Supplier, Other User	30 seconds	16 seconds		

4.11	4.11.2	Read Tariff (Secondary Element)	Import Supplier, Other User	30 seconds	n/a		Users may only be Eligible Users for this Service in respect of SMETS2+ Devices
4.12	4.12.1	Read Maximum Demand Import Registers	Import Supplier, Electricity Distributor	24 hours	n/a		Users may only be Eligible Users for this Service in respect of SMETS2+ Devices
4.12	4.12.2	Read Maximum Demand Export Registers	Export Supplier, Electricity Distributor	24 hours	n/a		Users may only be Eligible Users for this Service in respect of SMETS2+ Devices
4.13	4.13	Read Prepayment Configuration	Import Supplier Gas Supplier	30 seconds	16 seconds		
4.14	4.14	Read Prepayment Daily Read Log	Import Supplier Gas Supplier	30 seconds	n/a		Where a change of supplier occurs on any day, both the new supplier and the old supplier will be eligible to retrieve the daily read log for that day. Users may only be Eligible Users for this Service in respect of SMETS2+ Devices
4.15	4.15	Read Load Limit Data	Import Supplier, Electricity Distributor	24 hours	24 hours		
4.16	4.16	Read Active Power Import	Import Supplier, Electricity Distributor	30 seconds	16 seconds		

4.17	4.17	Retrieve Daily Consumption Log	Import Supplier, Gas Supplier, Electricity Distributor, Gas Transporter, Other User	30 seconds	n/a		Users may only be Eligible Users for this Service in respect of SMETS2+ Devices
4.18	4.18	Read Meter Balance	Import Supplier, Gas Supplier	30 seconds	16 seconds		
5.1	5.1	Create Schedule	Import Supplier, Gas Supplier, Electricity Distributor, Gas Transporter, Export Supplier, Other User	24 hours	24 hours	✓	
5.2	5.2	Read Schedule	Import Supplier, Gas Supplier, Electricity Distributor, Gas Transporter, Export Supplier, Other User	24 hours	24 hours	✓	
5.3	5.3	Delete Schedule	Import Supplier, Gas Supplier, Electricity Distributor, Gas Transport	24 hours	24 hours	✓	

			er, Export Supplier, Other User				
6.2	6.2.1	Read Device Configuration (Voltage)	Import Supplier, Electricity Distributor, Registered Supplier Agent	30 seconds	16 seconds		
6.2	6.2.2	Read Device Configuration (Randomisation)	Import Supplier, Electricity Distributor, Registered Supplier Agent	30 seconds	n/a		Users may only be Eligible Users for this Service in respect of SMETS2+ Devices
6.2	6.2.3	Read Device Configuration (Billing Calendar)	Import Supplier, Gas Supplier, Registered Supplier Agent	30 seconds	16 seconds		
6.2	6.2.4	Read Device Configuration (Identity exc. MPXN)	Import Supplier, Export Supplier, Gas Supplier, Electricity Distributor, Gas Transporter, Registered Supplier Agent, Other User	30 seconds	16 seconds		
6.2	6.2.5	Read Device Configuratio	Import Supplier,	30 seconds	16 seconds		

		n (Instantaneous Power Thresholds)	Registered Supplier Agent				
6.2	6.2.7	Read Device Configuration (MPXN)	Import Supplier, Export Supplier, Gas Supplier, Electricity Distributor, Gas Transporter, Registered Supplier Agent, Other User	30 seconds	n/a		Users may only be Eligible Users for this Service in respect of SMETS2+ Devices
6.2	6.2.8	Read Device Configuration (Gas)	Gas Supplier, Registered Supplier Agent, Gas Transporter	30 seconds	16 seconds		
6.2	6.2.9	Read Device Configuration (Payment Mode)	Import Supplier, Gas Supplier, Registered Supplier Agent	30 seconds	16 seconds		
6.2	6.2.10	Read Device Configuration (Event and Alert behaviours)	Import Supplier, Gas Supplier, Electricity Distributor	30 seconds	n/a		Users may only be Eligible Users for this Service in respect of SMETS2+ Devices
6.4	6.4.1	Update Device Configuratio	Import Supplier	30 seconds	16 seconds		

		n (Load Limiting General Settings)					
6.4	6.4.2	Update Device Configuration (Load Limiting Counter Reset)	Import Supplier	30 seconds	16 seconds		
6.5	6.5	Update Device Configuration (Voltage)	Electricity Distributor	30 seconds	16 seconds		
6.6	6.6	Update Device Configuration (Gas Conversion)	Gas Supplier	24 hours	24 hours		
6.7	6.7	Update Device Configuration (Gas Flow)	Gas Supplier	24 hours	24 hours		
6.8	6.8	Update Device Configuration (Billing Calendar)	Import Supplier, Gas Supplier	30 seconds	16 seconds		
6.11	6.11	Synchronise Clock	Import Supplier, Gas Supplier	30 seconds	16 seconds		
6.12	6.12	Update Device Configuration (Instantaneous Power Threshold)	Import Supplier	30 seconds	16 seconds		

6.13	6.13	Read Event or Security Log	Import Supplier, Gas Supplier, Electricity Distributor, Gas Transporter, Registered Supplier Agent	30 seconds	16 seconds		
6.14	6.14.1	Update Device Configuration (Auxiliary Load Control Description)	Import Supplier	30 seconds	n/a		Users may only be Eligible Users for this Service in respect of SMETS2+ Devices
6.14	6.14.2	Update Device Configuration (Auxiliary Load Control Scheduler)	Import Supplier	30 seconds	n/a		Users may only be Eligible Users for this Service in respect of SMETS2+ Devices
6.14	6.14.3	Update Device Configuration (Auxiliary Controller Scheduler)	Import Supplier	30 seconds	n/a		Users may only be Eligible Users for this Service in respect of SMETS2+ Devices
6.15	6.15.1	Update Security Credentials (KRP)	Import Supplier, Gas Supplier, Electricity Distributor, Gas Transporter	30 seconds	16 seconds		
6.15	6.15.2	Update Security Credentials (Device)	Import Supplier, Gas Supplier	30 seconds	n/a		Users may only be Eligible Users for this Service in

							respect of SMETS2+ Devices
6.17	6.17	Issue Security Credentials	Import Supplier, Gas Supplier	24 hours	n/a		Users may only be Eligible Users for this Service in respect of SMETS2+ Devices
6.18	6.18.1	Set Maximum Demand Configurable Time Period	Electricity Distributor	24 hours	n/a		Users may only be Eligible Users for this Service in respect of SMETS2+ Devices
6.18	6.18.2	Reset Maximum Demand Registers	Electricity Distributor	24 hours	n/a		Users may only be Eligible Users for this Service in respect of SMETS2+ Devices
6.20	6.20.1	Set Device Configuration (Import MPxN)	Import Supplier, Gas Supplier	30 seconds	n/a		Users may only be Eligible Users for this Service in respect of SMETS2+ Devices
6.20	6.20.2	Set Device Configuration (Export MPxN)	Export Supplier	30 seconds	n/a		Users may only be Eligible Users for this Service in respect of SMETS2+ Devices
6.21	6.21	Request Handover Of DCC Controlled Device Service Request	Import Supplier, Gas Supplier	30 seconds	16 seconds		
6.22	6.22	Configure Event Behaviour	Import Supplier, Gas Supplier, Electricity	30 seconds	n/a		Users may only be Eligible Users for this Service in respect of SMETS2+ Devices

			Distributor,				
6.23	6.23	Update Security Credentials (CoS)	Import Supplier, Gas Supplier	35 seconds	21 seconds		
6.24	6.24.1	Retrieve Device Security Credentials (KRP)	Import Supplier, Gas Supplier, Electricity Distributor, Gas Transporter	30 seconds	16 seconds		
6.24	6.24.2	Retrieve Device Security Credentials (Device)	Import Supplier, Gas Supplier	30 seconds	n/a		Users may only be Eligible Users for this Service in respect of SMETS2+ Devices
6.25	6.25	Set Electricity Supply Tamper State	Import Supplier	30 seconds	16 seconds		
6.26	6.26	Update Device Configuration (daily resetting of Tariff Block Counter Matrix)	Import Supplier	30 seconds	n/a		Users may only be Eligible Users for this Service in respect of SMETS2+ Devices
6.27	6.27	Update Device Configuration (RMS Voltage Counter Reset)	Electricity Distributor	30 seconds	16 seconds		

6.28	6.28	Set CHF Sub GHz Configuration	Import Supplier, Gas Supplier	30 seconds	n/a		Users may only be Eligible Users for this Service in respect of SMETS2+ Devices
6.29	6.29	Request CHF Sub GHz Channel Scan	Import Supplier, Gas Supplier	30 seconds	n/a		Users may only be Eligible Users for this Service in respect of SMETS2+ Devices
6.30	6.30	Read CHF Sub GHz Configuration	Import Supplier, Gas Supplier, Registered Supplier Agent	30 seconds	n/a		Users may only be Eligible Users for this Service in respect of SMETS2+ Devices
6.31	6.31	Read CHF Sub GHz Channel	Import Supplier, Gas Supplier, Registered Supplier Agent	30 seconds	n/a		Users may only be Eligible Users for this Service in respect of SMETS2+ Devices
6.32	6.32	Read CHF Sub GHz Channel Log	Import Supplier, Gas Supplier, Registered Supplier Agent	30 seconds	n/a		Users may only be Eligible Users for this Service in respect of SMETS2+ Devices
7.1	7.1	Enable Supply	Import Supplier	30 seconds	16 seconds		
7.2	7.2	Disable Supply	Import Supplier, Gas Supplier	30 seconds	16 seconds		
7.3	7.3	Arm Supply	Import Supplier,	30 seconds	16 seconds		

			Gas Supplier				
7.4	7.4	Read Supply Status	Import Supplier, Gas Supplier, Electricity Distributor, Gas Transporter, Export Supplier, Registered Supplier Agent	30 seconds	16 seconds		
7.5	7.5	Activate Auxiliary Load	Import Supplier	30 seconds	n/a		Users may only be Eligible Users for this Service in respect of SMETS2+ Devices
7.6	7.6	Deactivate Auxiliary Load	Import Supplier	30 seconds	n/a		Users may only be Eligible Users for this Service in respect of SMETS2+ Devices
7.7	7.7	Read Auxiliary Load Control Switch Data	Import Supplier, Electricity Distributor, Other User	30 seconds	n/a		Users may only be Eligible Users for this Service in respect of SMETS2+ Devices
7.8	7.8	Reset Auxiliary Load	Import Supplier	30 seconds	n/a		Users may only be Eligible Users for this Service in respect of SMETS2+ Devices
7.9	7.9	Add Auxiliary Load To Boost Button	Import Supplier	30 seconds	n/a		Users may only be Eligible Users for this Service in respect of SMETS2+ Devices

7.10.	7.10.	Remove Auxiliary Load From Boost Button	Import Supplier	30 seconds	n/a		Users may only be Eligible Users for this Service in respect of SMETS2+ Devices
7.11	7.11	Read Boost Button Details	Import Supplier, Other User	30 seconds	n/a		Users may only be Eligible Users for this Service in respect of SMETS2+ Devices
7.12	7.12	Set Randomised Offset Limit	Import Supplier	24 hours	n/a		Users may only be Eligible Users for this Service in respect of SMETS2+ Devices
7.13	7.13	Set Auxiliary Controller State	Import Supplier	30 seconds	n/a		Users may only be Eligible Users for this Service in respect of SMETS2+ Devices
7.14	7.14	Read Auxiliary Controller Configuration Data	Import Supplier, Electricity Distributor, Other User	30 seconds	n/a		Users may only be Eligible Users for this Service in respect of SMETS2+ Devices
7.15	7.15	Read Auxiliary Controller Operational Data	Import Supplier, Electricity Distributor, Other User	30 seconds	n/a		Users may only be Eligible Users for this Service in respect of SMETS2+ Devices
7.16	7.16	Limit APC Level	None	n/a	n/a		Not used
8.1	8.1.1	Commission Device	Import Supplier, Gas Supplier	30 seconds	16 seconds		

8.2	8.2	Read Inventory	Import Supplier, Gas Supplier, Electricity Distributor, Gas Transporter, Export Supplier, Registered Supplier Agent, Other User	30 seconds	16 seconds	✓	
8.3	8.3	Decommission Device	Import Supplier, Gas Supplier	30 seconds	16 seconds	✓	
8.4	8.4	Update Inventory	Import Supplier, Gas Supplier, Registered Supplier Agent, Electricity Distributor, Gas Transporter, Export Supplier, Other User	30 seconds	16 seconds	✓	Where a Device has an SMI Status of 'pending' only the User that added the Device to the Smart Metering Inventory may either update the details of that Device, or delete that Device from the Smart Metering Inventory. For Devices with an SMI Status other than 'pending', only the Responsible Supplier may amend the SMI Status of that Device.
8.5	8.5	Service Opt Out	None	n/a	n/a		Not used
8.6	8.6	Service Opt In	None	n/a	n/a		Not used

8.7	8.7.1	Join Service (Critical)	Import Supplier, Gas Supplier	30 seconds	16 seconds		
8.7	8.7.2	Join Service (Non-Critical)	Import Supplier, Gas Supplier, Other User	30 seconds	16 seconds		1. The only Devices that Other Users may join are Type 2 Devices that are not IHDs 2. Where a Gas Proxy Function is to be joined to a Gas Smart Meter, any Gas Supplier or Import Supplier that is a Responsible Supplier for any Device which is associated with the same Communications Hub Function as the Gas Proxy Function may request this Join Service Request.
8.8	8.8.1	Unjoin Service (Critical)	Import Supplier, Gas Supplier	30 seconds	16 seconds		

8.8	8.8.2	Unjoin Service (Non-Critical)	Import Supplier, Gas Supplier, Other User	30 seconds	16 seconds		1. The only Devices that Other Users may unjoin are Type 2 Devices that are not IHDs 2. Where a Gas Proxy Function is to be unjoined from a Gas Smart Meter, any Gas Supplier or Import Supplier who is a Responsible Supplier for any Device which is associated with the same Communications Hub Function as the Gas Proxy Function may request this Unjoin Service Request.
8.9	8.9	Read Device Log	Import Supplier, Gas Supplier, Other User	30 seconds	16 seconds		

8.11	8.11	Update HAN Device Log	Import Supplier, Gas Supplier, Other User	30 seconds	16 seconds		Other Users may only add (or remove) Type 2 Devices that are not IHDs to (or from) a HAN Device Log.
8.12	8.12.1	Restore HAN Device Log	Import Supplier, Gas Supplier	30 seconds	n/a		Users may only be Eligible Users for this Service in respect of SMETS2+ Devices
8.12	8.12.2	Restore GPF Device Log	Import Supplier, Gas Supplier	30 seconds	n/a		Any Gas Supplier or Import Supplier who is a Responsible Supplier for any Device which is associated with the same Communications Hub Function as the relevant Gas Proxy Function may request this Restore GPF Device Log Service Request. Users may only be Eligible Users for this Service in respect of SMETS2+ Devices
8.13	8.13	Return Local Command Response	Import Supplier, Gas Supplier	30 seconds	n/a		Users may only be Eligible Users for this Service in respect of SMETS2+ Devices
8.14	8.14.1	Communications Hub Status Update-CHF Install Success SM WAN	Import Supplier, Gas Supplier,	30 seconds	n/a	✓	Users may only be Eligible Users for this Service in respect of SMETS2+ Devices

8.14	8.14.2	Communications Hub Status Update-CHF Install Success No SM WAN	Import Supplier, Gas Supplier	30 seconds	n/a	✓	Users may only be Eligible Users for this Service in respect of SMETS2+ Devices
8.14	8.14.3	Communications Hub Status Update. – Fault Return	Import Supplier, Gas Supplier, Registered Supplier Agent	30 seconds	n/a	✓	Users may only be Eligible Users for this Service in respect of SMETS2+ Devices
8.14	8.14.4	Communications Hub Status Update – No Fault Return	Import Supplier, Gas Supplier, Registered Supplier Agent	30 seconds	n/a	✓	Users may only be Eligible Users for this Service in respect of SMETS2+ Devices
9.1	9.1	Request Customer Identification Number	Other User	30 seconds	n/a		Users may only be Eligible Users for this Service in respect of SMETS2+ Devices
11.1	11.1	Update Firmware	Import Supplier, Gas Supplier	24 hours	24 hours	✓	In respect of SMETS2+ Devices the DCC must ensure that the associated firmware update has been delivered to all relevant Communications Hub Functions within 5 days of receipt of the Service Request.
11.2	11.2	Read Firmware Version	Import Supplier, Gas Supplier,	30 seconds	16 seconds		

			Electricity Distributor, Gas Transporter, Export Supplier, Registered Supplier Agent, Other User				
11.3	11.3	Activate Firmware	Import Supplier, Gas Supplier	30 seconds	5 days		
11.4	11.4	Update PPMID Firmware	Import Supplier, Gas Supplier	24 hours	n/a	✓	In respect of SMETS2+ Devices the DCC must ensure that the associated firmware update has been delivered to all relevant Communications Hub Functions within 5 days of receipt of the Service Request.
12.1	12.1	Request WAN Matrix	Import Supplier, Gas Supplier, Registered Supplier Agent, Export Supplier, Electricity Distributor, Gas Transporter, Other User	30 seconds	n/a	✓	Users may only be Eligible Users for this Service in respect of SMETS2+ Devices
12.2	12.2	Device Pre-notification	Import Supplier, Gas	30 seconds	16 seconds	✓	

			Supplier, Registered Supplier Agent, Electricity Distributor, Gas Transporter, Export Supplier, Other User				
14.1	14.1	Record Network Data (GAS)	Gas Transporter	30 seconds	n/a		Users may only be Eligible Users for this Service in respect of SMETS2+ Devices

1 For the purposes of Section H3.11 (Categories of Service), Scheduled Services, On-Demand Services and Future-Dated Services are identified in the DCC User Gateway Interface Specification.

2 For Future-Dated Services, the Target Response Time shall be 30 seconds for an Update Security Credentials (COS) Service Request and shall be 24 hours for any other Service Request.

3 For Scheduled Services, the Target Response Time shall always be 24 hours.

4 Subject to paragraphs 2 and 3 above, the Target Response Time for Service Responses shall be as set out in the table above, in the column headed “SMETS2+ Target Response Time” or “SMETS1 Target Response Time” (as applicable, depending upon the Device to which the Service Response relates). In respect of SMETS2+ Devices, the Target Response Time for Service Responses refers to the period starting as described in Section H3.14 and ending on provision of the Service Response to the User, but only counting the processing time between (1) the DCC User Interface to the Communications Hub (inclusive); and/or (2) the Communications Hub to the DCC User Interface (inclusive). In respect of SMETS1 Devices, the Target Response Time for Service Responses refers to the period starting as described in paragraph 5 and ending on provision of the Service Response to the User, but only counting the processing time between (1) the DCC User Interface to the DCC SMETS1 Processing Systems (inclusive); and/or (2) the DCC SMETS1 Processing Systems to the DCC User Interface (inclusive). For the purpose of which, the "DCC SMETS1 Processing Systems" are the DCC Systems used to process communications and data relating to SMETS1 Devices, but excluding the SMETS1 SM WAN.

5 In relation to SMETS1 Devices, the start of the period referred to in paragraph 4 shall be:

(a) for SMETS1 Service Requests that are not a Sequenced Service, a Future Dated Service or a Scheduled Service, the receipt by the DCC of the relevant Service Request over the User Interface;

(b) for Sequenced Service Requests, the receipt by the DCC Individual Live System referred to at paragraph (a) of the definition of DCC Live Systems of the communication upon which the Service Request is dependent;

(c) for Future Dated Services or for Scheduled Services, the time and date for execution specified in the Service Request received by the DCC; or

(d) for SMETS1 Alerts and S1SP Alerts, the point in time at which the DCC SMETS1 Processing Systems have available to them the information that means that the relevant alert should be sent.

6 In the table above, where a "✓" appears in the column headed "Non-Device Service Request", this indicates that the Service Request described is a Non-Device Service Request.

7 The column of the table above headed "Notes":

(a) sets out further restrictions on which Users are eligible to receive the Services (and the definition of Eligible User and Eligible User Role will be interpreted accordingly); and

(b) sets out further restrictions that may apply, depending on the Device Type, that may be the target of a Service Request of that type from particular Users.

8 For the avoidance of doubt, none of the Services described in this Appendix attract an Explicit Charge.

9 The Monthly Service Metrics and Monthly Service Thresholds (referred to in Section H3.24 for reporting) are as set out in the table below. These shall not apply in respect of SMETS1 Smart Metering Systems. Accordingly, SMETS1 Service Requests and SMETS1 Smart Metering Systems shall be excluded from each of the calculations set out below.

Monthly Service Metric applies to Users acting in the following User Roles**	Monthly Service Metric applies to Service Requests for the following Services	Monthly Service Metric (excluding SMETS1 Service Requests and SMETS1 SMS)	Monthly Service Threshold
Import Supplier Gas Supplier	3.1 Display Message	The total over month m and the previous eleven months of the number of Service Requests; divided by the User ASMS$_m$.	24
Import Supplier Gas Supplier Export Supplier	4.8 Read Profile Data	The number of Service Requests in month m; divided by the number of Smart Metering Systems for which that User is a Responsible Supplier on the 15th day of month m.	The number of days in month m
Import Supplier Gas Supplier	11.1 Send Firmware	The total over month m and the previous eleven months of the number of Service Requests; divided by the User ASMS$_m$.	6
Electricity Distributor Gas Transporter	4.8 Read Profile Data	The number of Service Requests in month m; divided by the number of Smart Metering Systems for which the User is the Electricity Distributor or Gas Transporter on the 15th day of month m.	10^(-3) x 48 x the number of days in month m

Electricity Distributor Gas Transporter	4.8 Read Profile Data	The total over month m and the previous eleven months of the number of Service Requests; divided by the User $ASMS_m$.	4
Electricity Distributor	4.10 Read Network Data	The number of Service Requests in month m; divided the number of Smart Metering System for which the User is the Electricity Distributor or Gas Transporter on the 15th day of month m.	10^(-3) x the number of days in month m
Electricity Distributor	4.10 Read Network Data	The total over month m and the previous eleven months of the number of Service Requests; divided by the User $ASMS_m$.	4
Import Supplier Gas Supplier	11.4 Update PPMID Firmware	The total over month m and the previous eleven months of the number of Service Requests; divided by the User $ASMS_m$.	6

- In the above table, "User ASMSm" is determined in relation to each User and each month m as the mean of the numbers of Smart Metering Systems (excluding SMETS1 SMS) for which that User is a Responsible Supplier, Electricity Distributor or Gas Transporter (as applicable) on the 15th day of month m and on the 15th day of each of the previous 11 months.

- For each User, the "First Service Month" shall by the month following the month in which that User first sends a Service Request (of any type, but excluding SMETS1 Service Requests). No Monthly Service Metric shall be determined for a User in relation to any month prior to that User’s First Service Month.

- Where a Monthly Service Metric is to be determined for a User which includes a requirement to determine the number of Service Requests of a particular type sent over a time period which includes any time prior to that User’s First Service Month then:

  - the Monthly Service Metric for that User shall be the value determined in accordance with the table above, multiplied by twelve and divided by the number of months in that time period from (and including) the First Service Month; and

  - for the purposes of determining User ASMSm any months prior to the First Service Month shall be disregarded.

Version 1.0

APPENDIX F – MINIMUM COMMUNICATION SERVICES FOR SMETS1 METERS

Ref	Description	Eligible Users
1.1	Update Import Tariff (prepayment)	Import Supplier, Gas Supplier
1.1	Update Import Tariff (credit)	Import Supplier, Gas Supplier
1.2	Update Price (prepayment)	Import Supplier, Gas Supplier
1.2	Update Price (credit)	Import Supplier, Gas Supplier
1.5	Update Balance	Import Supplier, Gas Supplier
1.6	Update Payment Mode	Import Supplier, Gas Supplier
2.1	Update Prepay Configuration	Import Supplier, Gas Supplier
2.2	Top Up Device	Import Supplier, Gas Supplier
2.3	Update Debt	Import Supplier, Gas Supplier
2.5	Activate Emergency Credit	Import Supplier, Gas Supplier
3.2	Restrict Access – CoT	Import Supplier, Gas Supplier
3.3	Clear Event Log	Import Supplier, Gas Supplier
4.1	Read Instantaneous Import Register Values	Import Supplier, Gas Supplier, Electricity Distributor, Gas Transporter
4.2	Read Instantaneous Export Register Values	Export Supplier, Electricity Distributor
4.3	Read Instantaneous Prepayment Register Values	Import Supplier, Gas Supplier
4.4	Retrieve Billing Data Log	Import Supplier, Gas Supplier

4.8	Read Profile Data	Import Supplier, Gas Supplier, Electricity Distributor, Gas Transporter, Export Supplier, Other User
4.10	Read Network Data	Import Supplier, Gas Supplier, Electricity Distributor, Gas Transporter
4.11	Read Tariff	Import Supplier, Gas Supplier, Other User
4.16	Read Active Power Import	Import Supplier, Electricity Distributor
6.2	Read Device Configuration	Import Supplier, Gas Supplier, Electricity Distributor, Gas Transporter, Export Supplier, Registered Supplier Agent, Other User
6.4	Update Device Configuration (Load Limiting)	Import Supplier, Gas Supplier
6.5	Update Device Configuration (Voltage)	Electricity Distributor
6.6	Update Device Configuration (Gas Conversion)	Gas Supplier
6.7	Update Device Configuration (Gas Flow)	Gas Supplier
6.8	Update Device Configuration (Billing Calendar)	Import Supplier, Gas Supplier
6.11	Synchronise Clock	Import Supplier, Gas Supplier
6.12	Update Device Configuration (Instantaneous Power Threshold)	Import Supplier, Gas Supplier
6.13	Read Event or Security Log	Import Supplier, Gas Supplier, Electricity Distributor, Gas Transporter, Registered Supplier Agent
6.15	Update Security Credentials	Import Supplier, Gas Supplier, Electricity Distributor, Gas Transporter
6.23	Update Security Credentials (CoS)	Import Supplier, Gas Supplier
7.1	Enable Supply	Import Supplier
7.2	Disable Supply	Import Supplier, Gas Supplier

7.3	Arm Supply	Import Supplier, Gas Supplier
7.4	Read Supply Status	Import Supplier, Gas Supplier, Electricity Distributor, Gas Transporter, Export Supplier, Registered Supplier Agent
11.1	Update Firmware	Import Supplier, Gas Supplier
11.2	Read Firmware Version	Import Supplier, Gas Supplier, Electricity Distributor, Gas Transporter, Export Supplier, Registered Supplier Agent, Other User

Version G 3.0

Appendix G

DCC Gateway Connection Code of Connection

DEFINITIONS

Connection Period	means the period for which a DCC Gateway Connection is to be provided, as determined in accordance with the provisions of clause 1.6 of this document or pursuant to section H15.18(c) of the Code.
Contractual Bandwidth	means, in relation to any particular DCC Gateway HV Connection, the maximum number of megabits of data that are permitted to be transmitted each second over that connection.
DCC Gateway Connection Performance Report	means a monthly report relating to the performance of a DCC Gateway Connection containing the information set out in clauses 1.29 to 1.31 of this document.
Electronic Site Review	means a remote, desk-based assessment of the location at which the DCC Gateway Connection is required to assess whether a physical Site Survey is required.
Enabling Works	means any building or civil works, including laying of cables and gaining the necessary wayleaves or consents, required to be undertaken by a DCC Gateway Party and/or the DCC, to enable the DCC to provide a DCC Gateway Connection.
Inbound	means ‘to the DCC Gateway Equipment’.
Load	means the number of bits transferred in a given interval divided by the duration of that interval, expressed in bits per second.
Maximum Physical Bandwidth	means 100 megabits per second (Mbps) or such increases as may be notified to DCC Gateway Parties by the DCC from time to time.
Outbound	means ‘from the DCC Gateway Equipment’.
Site Survey	means a physical assessment of the location at which the DCC Gateway Connection is required, to assess whether any Enabling Works are required inside and/or outside the DCC Gateway Party’s premises and to detail preparatory works to be carried out by the DCC Gateway Party to be reflected in the offer made pursuant to section H15.12 of the Code.

1. DCC GATEWAY CONNECTIONS

1.1 Section H15 sets out principal rights and obligations applying to the provision of DCC Gateway Connections which are supplemented by the provisions set out below.

General Obligations

1.2 A DCC Gateway LV Connection will provide a download bandwidth of up to 40Mbps and an upload bandwidth of up to 10Mbps or such increases as may be notified to DCC Gateway Parties by the DCC from time to time.

1.3 A DCC Gateway HV Connection will provide a bandwidth of up to the Maximum Physical Bandwidth, which can be specified in increments of 10Mbps.

1.4 Each Party that wishes to establish a DCC Gateway Connection shall submit a request for a connection. Such request shall specify the DCC Gateway Bandwidth Option and:

(a) in the case of a request for a DCC Gateway LV Connection, the Connection Period; or

(b) in the case of a request for a DCC Gateway HV Connection;

(i) the required Contractual Bandwidth in relation to that connection, provided that the Contractual Bandwidth for any connection shall be an integer multiple of 10Mbps, and shall not exceed the Maximum Physical Bandwidth;

(ii) and the Connection Period; and

shall be made using the application form for such requests as published on the DCC Website.

1.5 Following a request for a connection being submitted, the DCC and the Party that submitted the request shall inform each other of the contact details of one or more persons working for their respective organisations for the purposes of communications associated with the establishment and management of DCC Gateway Connection(s). The following information shall be provided in relation to each such person (and shall subsequently be kept up to date by the providing Party):

(a) contact name;

(b) contact email;

(c) contact telephone;

(d) contact role(s);

(e) contact address;

and any other contact details as may be reasonably required by the DCC or the other Party from time to time.

Connection Mechanisms and Period of Connection

1.6 Where a DCC Gateway Party wishes to procure a DCC Gateway Connection:

(a) the connection may be requested for an initial period of either one or three years from the point at which the connection becomes capable of operation; and

(b) the DCC shall notify the DCC Gateway Party when the connection becomes capable of operation.

1.7 Where a DCC Gateway Party requests multiple DCC Gateway Connections for a single location at the same time, the DCC shall take all reasonable steps to conduct any Site Surveys in a single visit to that location.

1.8 Where any Enabling Works are required, the DCC Gateway Party and the DCC shall inform each other of the progress and completion of the Enabling Works.

1.9 In the event that a DCC Gateway Party wishes to decrease the Contractual Bandwidth of its DCC Gateway HV Connection during its Connection Period:

(a) the DCC Gateway Party shall inform the DCC, provided that the requested decrease shall be an integer multiple of 10Mbps;

(b) the DCC shall reduce the Contractual Bandwidth accordingly as soon as is reasonably practicable and in any event within 30 days of being informed of the required adjustment; and

(c) the DCC shall provide the DCC Gateway Party with advance notice of the date from which the adjusted Contractual Bandwidth shall take effect.

1.10 In the event that a DCC Gateway Party wishes to increase the Contractual Bandwidth of its DCC Gateway HV Connection during its Connection Period:

(a) the DCC Gateway Party shall inform the DCC, provided that the requested increase shall be an integer multiple of 10Mbps, and shall not exceed the Maximum Physical Bandwidth of that connection;

(b) the DCC shall confirm to the DCC Gateway Party the applicable charges arising from the increase as soon as reasonably practicable and in any event within 5 Working Days;

(c) following notification of the applicable charges, the DCC Gateway Party shall, within 30 days, confirm to the DCC that the DCC Gateway Party wishes to proceed with the increase (and where no such confirmation is provided within 30 days, the DCC's offer to increase the bandwidth at the notified applicable charge shall lapse);

(d) where the DCC receives confirmation from the DCC Gateway Party within 30 days that it wishes to proceed with the increase, the DCC shall increase the Contractual Bandwidth accordingly as soon as is reasonably practicable and in any event within 30 days of receiving such confirmation; and

(e) the DCC shall provide the DCC Gateway Party with advance notice of the date from which the adjusted Contractual Bandwidth shall take effect.

Installation, Maintenance and Removal of DCC Gateway Equipment

1.11 Sections H15.20 to H15.28 set out principal rights and obligations relating to DCC Gateway Equipment which are supplemented with the provisions set out below.

1.12 Where the DCC is undertaking works at the DCC Gateway Party's premises for the purposes of installation, maintenance or removal of DCC Gateway Equipment, the DCC shall take all reasonable steps to avoid interrupting the DCC Gateway Party's existing telecommunications services at those premises. In the event that it is necessary to interrupt the DCC Gateway Party's existing telecommunications services:

(a) the DCC shall take all reasonable steps to provide the DCC Gateway Party with advance notice of the interruption; and

(b) the DCC Gateway Party shall have the right to request that such interruption be rescheduled, such request not to be unreasonably withheld or delayed by the DCC.

1.13 Where the DCC Gateway Party's existing telecommunications services are interrupted as a result of DCC undertaking works as set out in clause 1.12, the DCC shall:

(a) take all reasonable steps to minimise the length and impact of the interruption; and

(b) ensure that the telecommunications services are restored as soon as is reasonably practicable and in any event immediately following the completion of the works.

1.14 Where maintenance undertaken by the DCC requires the replacement of DCC Gateway Equipment:

(a) the DCC shall remove that equipment within 30 days of the date of the replacement activity; and

(b) in the event that such equipment is not removed within 30 days, the DCC Gateway Party may dispose of the equipment and shall notify the DCC at least 5 days prior to disposing of the DCC Gateway Equipment, provided that the DCC shall have the right to remove the equipment prior to the end of that 5 day period.

1.15 Subject to the obligations in Sections H15.20, H15.21, and H15.28(b) for the DCC to act in accordance with Good Industry Practice, the DCC shall not be responsible for or liable to the DCC Gateway Party for making good any minor repairs to decoration that have become necessary as a result of the DCC's installation, maintenance or removal of DCC Gateway Equipment.

1.16 Each DCC Gateway Party shall make available to the DCC all information, facilities and services reasonably required by the DCC to carry out installation, maintenance or removal of DCC Gateway Equipment.

1.17 Where reasonably requested by a DCC Gateway Party, the DCC shall provide such information as required by the DCC Gateway Party in order to facilitate the installation, maintenance or removal of DCC Gateway Equipment. Following receipt of that information, the DCC Gateway Party shall have the right to reschedule the visit by the DCC. The DCC Gateway Party acknowledges that rescheduling of the visit required for installation may give rise to the DCC notifying a revised connection date pursuant to H15.15 and that rescheduling the visit for maintenance or removal may give rise to corresponding delays for the completion of that maintenance or removal.

1.18 Subject to Section H15.24, and except where such steps are necessary on security or safety grounds, each DCC Gateway Party shall not take any steps that may affect the operation of the DCC Gateway Connection without prior agreement of the DCC, such agreement not to be unreasonably withheld or delayed, and shall ensure that no person other than the DCC undertakes any maintenance of the DCC Gateway Equipment.

1.19 The DCC Gateway Party shall implement and maintain controls to ensure the physical security of the DCC Gateway Equipment, including that only appropriately authorised persons have access to such equipment, and that this access is recorded in a log maintained for that purpose.

1.20 The DCC shall take all reasonable steps to comply with any DCC Gateway Party's reasonable requests in respect of installation or relocation of DCC Gateway Equipment. The DCC Gateway Party shall be entitled to make the final decision on the routing of cables and location of the DCC Gateway Equipment, subject to such decision not impacting on the DCC's ability to provide and maintain the DCC Gateway Connection.

1.21 The DCC may modify or replace the DCC Gateway Equipment where necessary to maintain the operation of the DCC Gateway Connection, provided that such modification or replacement does not materially diminish the performance of the DCC Gateway Connection, and only after giving reasonable notice of the need to modify or replace the DCC Gateway Equipment to the DCC Gateway Party.

1.22 The DCC shall wherever possible carry out maintenance of the DCC Gateway Equipment installed at a DCC Gateway Party's site remotely, using the network connection itself to gain access to the DCC Gateway Equipment:

(a) where reasonably practicable, the DCC shall provide reasonable advance notice to the DCC Gateway Party of such maintenance;

(b) such advance notice shall be provided to a contact nominated to the DCC for that purpose by the DCC Gateway Party, or otherwise the contact provided pursuant to clause 1.5; and

(c) the DCC Gateway Party shall have the right to request that the maintenance is rescheduled, such request not to be unreasonably withheld or delayed by the DCC.

1.23 The DCC and each DCC Gateway Party shall provide sufficient information to each other to enable the establishment and maintenance of the network layer connectivity across the DCC Gateway Connection.

1.24 The DCC shall give the DCC Gateway Party reasonable notice of required site visits to perform installation, maintenance or removal of DCC Gateway Equipment and the DCC shall accommodate the DCC Gateway Party's reasonable requests regarding the timing of such visits.

Reporting Obligations

1.25 Where a DCC Gateway Party notifies the DCC that the DCC Gateway Party wishes to receive DCC Gateway Connection Performance Reports, the DCC shall provide such DCC Gateway Connection Performance Reports, in accordance with clause 1.26, until notified by the DCC Gateway Party that it no longer wishes to receive such reports. The DCC shall notify DCC Gateway Parties of the DCC contact details for these purposes.

1.26 By the end of the 10th Working Day following the end of each calendar month, the DCC shall provide each DCC Gateway Party who has requested a report pursuant to clause 1.25 with a DCC Gateway Connection Performance Report for each of their DCC Gateway Connections for the previous calendar month (the 'reporting period').

1.27 The DCC shall provide DCC Gateway Connection Performance Reports to DCC Gateway Parties via an appropriate mechanism (as reasonably determined by the DCC) and notify each DCC Gateway Party of such mechanism. Where the DCC first proposes a mechanism or proposes to change the mechanism for the provision of the DCC Gateway Connection Performance Reports, the DCC shall:

(a) undertake reasonable consultation with DCC Gateway Parties regarding the proposed mechanism or the proposed modification thereto;

(b) give due consideration to, and take into account, any consultation responses received;

(c) publish a statement of its reasons for proposing or modifying the mechanism, as applicable, together with copies of any consultation responses received; and

(d) provide reasonable notice to DCC Gateway Parties of the mechanism or any changes in the mechanism, as applicable.

1.28 The DCC shall ensure that each DCC Gateway Connection Performance Report is made available to be accessed (via the mechanism described in clause 1.27) by the relevant DCC Gateway Party at any time in the six month period following the provision of the report.

1.29 The DCC shall ensure that each DCC Gateway Connection Performance Report shall include values for each of the data elements set out in Table 1 (DCC Gateway Connection performance measures) in respect of the performance of the relevant DCC Gateway Connection during the reporting period.

1.30 The DCC shall ensure that each DCC Gateway Connection Performance Report is provided in a Portable Document Format (PDF).

1.31 The DCC shall provide the data (recorded in per minute intervals) used to calculate the values for each of the data elements set out in Table 1in a separate file in Comma Separated Variable (CSV) format except those data that relate to:

(a) changes in values between the relevant reporting period and the preceding reporting period;

(b) calculation of Jitter and Latency (as defined in Table 1 below); and

(c) outages and availability (as defined in Table 1 below).

Table 1: DCC Gateway Connection performance measures

Data element	**Description**
95th percentile Load Inbound	Load Inbound values for each minute during the reporting period shall be ranked from highest to lowest and the top five percent shall be discarded. The highest value of those which remain shall be the 95th percentile Load Inbound.
95th percentile Load Outbound	Load Outbound values for each minute during the reporting period shall be ranked from highest to lowest and the top five percent shall be discarded. The highest value of those which remain shall be the 95th percentile Load Outbound.
95th percentile utilisation Inbound	The 95th percentile Load Inbound as a proportion of the Contractual Bandwidth, expressed as a percentage.
95th percentile utilisation Outbound	The 95th percentile Load Outbound as a proportion of the Contractual Bandwidth, expressed as a percentage.

Availability	The percentage of time for which the DCC Gateway Equipment or the network used by the DCC to transfer data to or from the DCC Gateway Equipment, was available during the reporting period.
Average Load Inbound	The mean value of Load Inbound during the reporting period.
Average Load Outbound	The mean value of Load Outbound during the reporting period.
Average utilisation Inbound	The mean Load Inbound during the reporting period as a proportion of the Contractual Bandwidth, expressed as a percentage.
Average utilisation Outbound	The mean Load Outbound during the reporting period as a proportion of the Contractual Bandwidth, expressed as a percentage.
Change in the 95th percentile Load	The difference in the 95th percentile Load Inbound or Outbound between the reporting period and the preceding reporting period, whichever difference is greater (the highest absolute value, ignoring the sign), as a proportion of the equivalent Load for the preceding reporting period, expressed as a percentage.
Change in volume	The difference in the total amount of data transferred Inbound or Outbound between the reporting period and the preceding reporting period, whichever difference is greater (the highest absolute value, ignoring the sign), as a proportion of the equivalent value for the preceding reporting period, expressed as a percentage.
Discards	The total number of data packets not delivered due to network routing issues during the reporting period.
Errors	The total number of data packets where discrepancies were identified during transmission in the reporting period, expressed as a percentage.
Jitter	The time, in milliseconds, measuring the variation in latency. The interval over which the variation is measured is determined in accordance with Good Industry Practice.
Latency	The time, in milliseconds, taken for a test ping to be transferred Inbound and Outbound.
Outages	The total time, in minutes, for which the DCC Gateway Equipment or the network used by the DCC to transfer data to or from the DCC Gateway Equipment was not available during the reporting period.
Peak Load Inbound	The highest single value of Load Inbound during the reporting period.

Peak Load Outbound	The highest single value of Load Outbound during the reporting period.
Peak utilisation Inbound	The peak Load Inbound during the reporting period as a proportion of the Contractual Bandwidth, expressed as a percentage.
Peak utilisation Outbound	The peak Load Outbound during the reporting period as a proportion of the Contractual Bandwidth, expressed as a percentage.
Volume Inbound	The total amount of data Inbound during the reporting period, expressed in bytes.
Volume Outbound	The total amount of data Outbound during the reporting period, expressed in bytes.

Version H 3.0

APPENDIX H

CH Handover Support Materials

Definitions

Advanced Shipment Notification (or ASN)	means, in relation to a Region, the notification containing the information listed in Annex A of this document under ‘Advanced Shipment Notification’ identified as being provided in relation to that Region.
Cellular Communications Hub	means a WAN Variant in the Central Region and the South Region which is capable of using mobile cellular radio technology to connect to the SM WAN.
Central Region	means the Region which covers the majority of Wales and the majority of central England.
CH Delivery and Returns	means the OMS Account profile which enables the user of an OMS Account with this profile or the DCC on their behalf to carry out the following activities on the OMS: a. the viewing and amendment of Communication Hub Consignments; b. the viewing and downloading of Advanced Shipment Notifications; c. the creation, acceptance and rejection of requests to return Communications Hubs and Communications Hub Auxiliary Equipment to the DCC; and d. the maintenance of Delivery Location information and Party contact details in relation to Communications Hub Orders.
CH Ordering	means the OMS Account profile which enables the user of an OMS Account with this profile or the DCC on their behalf to carry out the following activities on the OMS: a. the creation, submission, viewing, and amendment of Communications Hub Forecasts, Communications Hub Orders; b. the creation of Delivery Location information; and c. all activities that can be carried out under an OMS Account with the CH Delivery and Returns profile.
CH Supporting Information	means the materials identified as such which: a. are published by the DCC on the DCC Website; and b. contain the information required by clause 1.4 of this document.
CH Query	means the OMS Account profile which enables the user of an OMS Account with this profile or the DCC on their behalf to carry out the following activities on the OMS: a. the viewing of Communication Hub Consignments, Communications Hub Forecasts, Communications Hub Orders; and b. the viewing and downloading of Advanced Shipment Notifications.
CHF Identifier	has the meaning given to that term in the CHTS.
Communications Hub Variants	means variations of Communications Hubs describing their HAN and WAN communications characteristics.

Communications Hub Transfer Reference	means a reference that is unique to a Communications Hub Transfer and which is first notified as set out in clause 9.1.
Coverage Area	means the geographical coverage of the SM WAN at a point in time.
Delivery Issues Report Notification (or DIRN)	means the report provided to a Party by the DCC pursuant to clause 6.23.
Delivery Note	means, in relation to a Region, the documentation containing the information listed in Annex A under 'Delivery Note' identified as being provided in relation to that Region.
Dual Band Communications Hub	a HAN Variant which is capable of using 2.4GHz and Sub GHz frequencies for communication on the Home Area Network (HAN).
GPF Identifier	has the meaning given to that term in the CHTS.
Installation Location	means the location of the premises at which a Communications Hub is planned to be, or has been, installed.
M1 Aerial Type	means the low gain mesh aerial type in the Central Region and the South Region further described in the Communications Hub Supporting Information and which may not be ordered by Parties but is supplied and fitted directly by DCC.
M2 Aerial Type	means the high-gain mesh aerial type in the Central Region and the South Region further described in the Communications Hub Supporting Information and which may not be ordered by Parties but is supplied and fitted directly by DCC.
Mesh Communications Hub	means a WAN Variant in the Central Region and the South Region which is capable of using both mobile cellular radio technology and wireless mesh radio technology to connect to the SM WAN.
North Region	means the Region which covers the majority of Scotland and the majority of northern England.
OMS Account	means an arrangement by which a user is given access to an OMS profile by entering a unique username and password.
OMS Order Reference	means a reference that is unique to a Communications Hub Order and which is first notified as set out in clause 3.19.
Order Management System (or **OMS)**	means the systems comprising part of the CH Ordering System and which are used for: a. the submission of information comprising Communications Hub Forecasts and Communications Hub Orders;

	b. the management and tracking of Communications Hub Orders and deliveries of Communications Hubs and Communications Hub Auxiliary Equipment; and c. the rejection, return or replacement of Communications Hubs and Communications Hub Auxiliary Equipment.
Significant Metallic Obstruction	has the meaning given to that term in the CH Installation and Maintenance Support Materials.
Single Band Communications Hub	means a HAN Variant which is only capable of using 2.4GHz frequency for communication on the Home Area Network (HAN).
South Region	means the Region which covers the majority of southern England.
Special Installation Mesh Communications Hub	means a WAN Variant in the Central Region and the South Region which provides two external aerial ports on the front face to enable connection of two external aerials – one cellular (either a T1 Aerial Type, T2 Aerial Type or T3 Aerial Type) and one mesh (either an M1 Aerial Type or M2 Aerial Type). This WAN variant may not be ordered by Parties but is supplied and fitted directly by DCC
T1 Aerial Type	means the low gain aerial type in the Central Region and the South Region further described in the Communications Hub Supporting Information and which do not comprise part of the Communications Hub and may be ordered as Communications Hub Auxiliary Equipment.
T2 Aerial Type	means the high gain aerial type in the Central Region and the South Region further described in the Communications Hub Supporting Information and which do not comprise part of the Communications Hub and may be ordered as Communications Hub Auxiliary Equipment.
T3 Aerial Type	means the high gain aerial type in the Central Region and the South Region further described in the Communications Hub Supporting Information and which may not be ordered by Parties but is supplied and fitted directly by DCC.
Transfer Note	means, in relation to a Communications Hub Transfer, the documentation containing the information listed in Annex A under 'Delivery Note' identified as being provided in relation to that transfer.
Transfer Window	means, in relation to a Communications Hub Transfer, the collection window (of at least four hours) on the Transfer Date, as agreed under Clause 9.
Working Hours	for the purposes of this document, means the period between 07:00 and 17:00 during a Working Day.

1. INTRODUCTION

Document purpose

1.1 This document is the CH Handover Support Materials, and forms Appendix H of the Code.

General clarifications

1.2 Unless expressly stated otherwise, the obligations in this document are applicable in relation to all Regions.

1.3 Unless expressly stated otherwise, none of the obligations in this document apply to Test Communications Hubs.

1.4 The DCC shall publish the CH Supporting Information on the DCC website, which shall include the following information:

(a) information regarding Advance Shipment Notification format for Communications Hubs and Aerial Types that can be ordered through OMS;

(b) additional diagrammatical information supporting the definition of Significant Metallic Obstruction;

(c) a description of the way in which LED indicators depict the operational status of a Communications Hub; and

(d) a description of the aerial types DCC makes available within the South Region and Central Region (T1 Aerial Type, T2 Aerial Type, T3 Aerial Type, M1 Aerial Type and M2 Aerial Type).

1.5 Prior to first publication of, and any subsequent modification to the CH Supporting Information the DCC shall:

(a) undertake reasonable consultation with Parties regarding its content or any proposed modification thereto;

(b) give due consideration to, and take into account, any consultation responses received; and

(c) publish a statement of its reasons for including or modifying content, as applicable, together with copies of any consultation responses received that are not marked as confidential.

1.6 The DCC shall publish the initial CH Supporting Information and any subsequently modified versions on the DCC Website as soon as reasonably practicable following the completion of the activities set out in clause 1.5.

2. ORDER MANAGEMENT SYSTEM

2.1 Subject to the remaining provisions set out in clauses 2.1 to 2.7 of this document, the DCC shall provide each Party with access to the Order Management System (OMS) for each Region via:

(a) the Self-Service Interface; and

(b) a public internet link.

Access to the OMS

2.2 A Party other than the DCC shall only access the OMS via an OMS Account.

2.3 Any Party first seeking to access the OMS for a Region shall submit a valid request for one or more OMS Accounts via the Service Desk.

2.4 Each Party may request access for OMS Accounts in relation to each Region. DCC shall provide four OMS Accounts per Region at no additional Charge. A Party may request more than four OMS Accounts per Region, subject to Section F5.23.

2.5 A request for an OMS Account shall be considered valid if it includes:

(a) the Party Signifier for the Party making the request;

(b) a username comprised of an email address for each OMS Account being requested, which shall not be used for any other accounts accessing the OMS for that Region;

(c) the OMS profile(s) to be associated with each OMS Account being requested; and

(d) the Region for which access is being requested.

2.6 The DCC shall provide a password to be associated with each individual OMS Account to the requesting Party no later than four Working Days following the receipt of a valid request for an OMS Account. The requesting Party may then use the combination of username and password to access the relevant instance of the OMS.

2.7 A Party may request a change to the OMS profile(s) that are available via an OMS Account, modify the OMS Account or close the OMS Account by submitting a request to the Service Desk. The DCC shall implement such a change no later than four Working Days following the receipt of such a request and shall notify the Party on the day of completion.

3. FORECASTING AND ORDERING COMMUNICATIONS HUBS

Communications Hub Forecasts

3.1 Following receipt of a Communications Hub Forecast or the deeming of a Communications Hub Forecast by the DCC in accordance with Section F5.6, the DCC shall notify via email to all OMS Accounts associated with that Party that the following information is available via the OMS:

(a) a unique reference for the relevant Communications Hub Forecast; and

(b) the associated date, which shall be:

(i) where a Communication Hub Forecast has been submitted by a Party, the date of submission; or

(ii) where the Communications Hub forecast has not been submitted by a Party, the date at which the DCC has deemed that forecast.

SM WAN coverage information

3.2 The DCC shall provide Parties with information regarding SM WAN coverage at potential Installation Locations and the WAN Variant (and, where applicable, the Communications Hub Auxiliary Equipment) required for each Installation Location via the SM WAN Coverage Database. The DCC shall make the SM WAN Coverage Database information available via:

(a) the Self Service Interface;

(b) responses to Service Request 12.1 (Request WAN matrix); or

(c) a reasonable alternative method, as specified by the DCC, where the methods specified in clauses 3.2(a), 3.2(b) are not available.

3.3 Where a Party requires SM WAN coverage information for an Installation Location where there is no associated postcode in DCC Systems, the Party may raise a Service Management Service Request with the DCC, and in so doing shall provide the geographic latitude and longitude, for the Installation Location. The DCC shall resolve the Service Management Service Request by providing SM WAN coverage information for the Installation Location to the Party which raised the matter, and by additionally allocating the Installation Location to a Region.

Delivery Locations

3.4 A Party shall provide Delivery Locations on the OMS using the CH Ordering profile and shall provide and maintain the following information for each Delivery Location:

(a) the full delivery address;

(b) operating hours; and

(c) the name, email address, and telephone number for a nominated contact in relation to Communications Hubs Orders.

3.5 The DCC shall ensure that the OMS allows each Party using the CH Ordering profile to select a maximum of two Delivery Locations for each Communications Hub Order.

Deemed Communications Hub Orders

3.6 Where, in accordance with Section F5.13(c), the DCC deems the quantities of Communications Hubs to be included in a Communications Hub Order for a Party, it shall inform via email notification to all OMS Accounts associated with that Party that a deemed order has been made and make available, via the OMS, details of the deemed quantity of each Device Model and of any Communications Hub Auxiliary Equipment.

3.7 Where a Party receives a notification in accordance with clause 3.6, that Party shall specify a Delivery Location or Delivery Locations for the Communications Hub Order within two Working Days and shall comply with, and provide the further information set out in, clauses 3.13 and 3.14.

3.8 Where a Party has not specified a Delivery Location or Delivery Locations, or provided the other information required, in accordance with clause 3.7, the DCC shall specify the Communications Hub Order Delivery Location or Delivery Locations using Delivery Locations provided for any previous orders and, specify the further information set out in, clauses 3.13 and 3.14.

3.9 Where the DCC has determined the Delivery Location(s) pursuant to clause 3.8 and the relevant Party has not notified the DCC within 30 days of the DCC's notification pursuant to clause 3.6, that the extant delivery details are correct, then the relevant Party shall be deemed to have requested cancellation of the

Consignment or Consignments (and Section F5.19 shall be deemed to apply). The DCC shall notify that such a request has been deemed, via an email to all OMS Accounts associated with that Party.

Submitting Communications Hub Orders

3.10 When submitting a Communications Hub Order, each Party shall ensure that only such Communications Hub Variants and Communications Hub Auxiliary Equipment are ordered as it may reasonably require to:

(a) complete planned installations using the WAN Variants and Communication Hub Auxiliary Equipment that are indicated as required for the relevant Installation Location(s) on the SM WAN Coverage Database;

(b) conform to the proportions of T1 Aerial Type and T2 Aerial Type estimated as necessary within the CH Supporting Information to provide for Mesh Communications Hub installations; and

(c) maintain sufficient stock to resolve coverage Incidents and Communication Hub faults as described in the CH Installation and Maintenance Support Materials.

3.11 Where a Party submits a Communications Hub Order for the Central Region or the South Region that results in greater than 10% of the total number of Communications Hubs in the Communications Hub Order being Mesh Communications Hubs, the DCC may request an explanation why the quantity of Mesh Communications Hubs ordered is required and where such an explanation is requested the Party shall provide the explanation via email promptly.

3.12 Each Party shall ensure that its Communications Hubs Order is such that it would not result in a requirement for the DCC to deliver a single Consignment that comprises only Communications Hub Auxiliary Equipment.

3.13 In addition to complying with the requirements set out in Section F5.8, for each Communications Hub Order that it submits, a Party shall:

(a) request delivery to no more than two Delivery Locations per Region;

(b) request delivery to each Delivery Location no more than once in any single week; and

(c) specify a Delivery Date and associated Delivery Window that is within Working Hours.

3.14 A Party submitting a Communications Hub Order shall ensure that for each delivery that will result from that Communications Hub Order and in relation to the Region to which the Order relates:

(a) the number of each Communications Hub Variant is an integer multiple of the quantity of Communications Hubs that are contained in a carton for that Communications Hub Variant, as specified in Annex B of this document;

(b) the total number of Communications Hubs ordered is such that a pallet layer contains the total number of cartons for that pallet layer as specified in Annex B of this document and only contains a single Communications Hub Variant; and

(c) the total number of Communications Hubs is greater than or equal to the quantity of Communications Hubs contained in a complete standard pallet, as specified in Annex B of this document.

3.15 The DCC shall package and load Communications Hubs as described in Annex D of this document.

3.16 The DCC shall make available to a Party via the CH Ordering System at least one contact telephone number and email address for the DCC which is relevant to each Communications Hub Order placed by that Party for the purposes of allowing a Party to request amendments to Delivery Locations, Delivery Dates, or Delivery Windows in relation to a Communications Hub Order that it has submitted.

3.17 A Party shall make available to the DCC via the CH Ordering System at least one contact telephone number and email address for that Party which is relevant to each of its Communications Hub Orders, which shall be used by the DCC for any email or telephone communications regarding the order.

3.18 For each Communications Hub Order, where the DCC identifies an opportunity for consolidation of a Party's Consignments into a single delivery vehicle, the DCC may request permission to amend a Communications Hub Order to enable such consolidation. The agreement of the Party to such a request shall not be unreasonably withheld.

Order Verification and Acceptance

3.19 The notification that the DCC is required to provide pursuant to Section F5.16 shall be provided by the DCC via email to all OMS Accounts associated with that Party notifying that information is available via the OMS. Such information will consist of the following;

(a) an OMS Order Reference; and

(b) confirmation that the Communications Hub Order is:

(i) compliant with the requirements of Section F5 (and therefore accepted without amendment); or

(ii) not compliant with the requirements of Section F5.

3.20 Where a notification has been made of the type set out in clause 3.19(b)(ii), the further notification that DCC is required to provide pursuant to Section F5.17 shall be provided by the DCC via email to all OMS Accounts associated with that Party notifying that information is available via the OMS. The information on the OMS shall state whether the Order is:

(a) accepted, in full and is not subject to amendment;

(b) accepted, in part or is subject to amendment; or

(c) rejected;

and in each case

(d) the reason for the decision.

3.21 In the event that a Party submits a Communications Hub Order, or subsequently seeks to amend that order pursuant to clause 4.3, that would result in one or more deliveries that do not meet the conditions set out in clause 3.12, 3.13 and 3.14, such an order shall be deemed to be a request for non-standard delivery instructions in accordance with Section F6.17.

3.22 Where a Party has or has been deemed to have requested non-standard delivery instructions, the DCC shall provide a non-binding estimate of any applicable Charge for that Communications Hub Order to that Party within five Working Days of receipt of such request.

3.23 On receipt of an estimate of the applicable non-standard delivery Charge pursuant to clause 3.22, the relevant Party shall, within five Working Days, either;

(a) leave the non-standard delivery order unchanged on the OMS, and therefore be deemed to have agreed to pay any applicable Explicit Charges pursuant to Sections F6.17 and K7.5(k); or

(b) amend the relevant Communications Hub Order via the OMS using the CH Ordering profile such that it no longer results in non-standard delivery instructions.

4. ORDER MANAGEMENT

Non-standard cancellation of Consignments

4.1 Pursuant to Section F5.19, a Party wishing to obtain an estimate of costs and expenses in relation to the cancellation of a Consignment shall submit a request for this estimate by contacting the Service Desk.

4.2 Where pursuant to Section F5.19 a Party wishes to cancel a Consignment, its notification to this effect must be provided to the Service Desk.

Delivery Date and Time Amendments

4.3 Following acceptance of a Communications Hub Order by the DCC, a Party may request amendments to the Delivery Date or Delivery Window for a Consignment up to 30 days prior to the original Delivery Date. Such requests shall be submitted via the OMS through a direct update to the order details using the CH Ordering profile.

4.4 Any request by a Party for an amendment pursuant to clause 4.3, in addition to the provisions in clauses 3.13 and 3.14, is subject to the following restrictions:

(a) the revised Delivery Date for a Consignment must be a Working Day within five days of the original Delivery Date and within the same Delivery Month; and

(b) the revised Delivery Window for a Consignment must be within Working Hours.

4.5 In the event that a Party wishes to request an amendment to the Delivery Date or Delivery Window for a Consignment within 30 days of the Delivery Date, or where the Party wishes to request an amendment to the Delivery Location because exceptional circumstances mean that delivery to the original specified Delivery Location is no longer practicable, that Party shall contact the DCC directly using the contact details set out in clause 3.16; in this event the restrictions as detailed in clause 4.4 shall apply and DCC may specify further reasonable restrictions which shall be notified via telephone or email and may deem such a request to be a request for non- standard delivery instructions.

4.6 Where the DCC deems such a request to be a request for non-standard delivery instructions, clause 3.22 shall apply. Upon receipt of an estimate of the applicable non-standard delivery Charge, the relevant Party shall, within five Working Days, either;

(a) leave the non-standard delivery order unchanged on the OMS, in which case, the Party shall be deemed to have withdrawn its request for an amendment pursuant to 4.5; or

(b) notify the DCC of its agreement to pay any applicable Explicit Charges pursuant to Sections F6.17 and K7.5(k) and the DCC shall update the OMS accordingly.

4.7 The DCC may consider an amendment to the Delivery Date or Delivery Window for a Consignment made within five Working Days of the Delivery Date, but shall not be obliged to do so.

4.8 Where the DCC has not deemed a request pursuant to clause 4.5 to be a request for non-standard delivery instructions, the DCC shall confirm acceptance of any request made by a Party in accordance with clause 4.5 and the DCC shall update the OMS to reflect the amendments agreed with the Party, as soon as is reasonably practical and in any event within five Working Days of the request having been made.

4.9 Where pursuant to clause 4.8 the DCC confirms to a Party that a change to the Delivery Date or Delivery Window, or Delivery Location is accepted; the DCC shall be obliged to deliver the Communications Hub Order in accordance with those updated instructions.

Monitoring Order Status

4.10 The DCC shall ensure that the following information is available to a Party via the OMS for all OMS Accounts associated with that Party in relation to each Communications Hub Order that it submitted in the previous 12 months:

(a) The Communications Hub Order status, being one of:

(i) Submitted – order submitted to the DCC;

(ii) Accepted – order (where appropriate, as amended) accepted by the DCC;

(iii) Rejected – full order rejected by DCC;

(iv) Partially Delivered – partial order delivered and accepted by the Party; or

(v) Delivered – all Consignments for the order accepted by the Party.

(b) the status of each Consignment within a Communications Hub Order, being one of:

(i) In Progress – Consignment scheduled for delivery within 30 days or less;

(ii) Shipped - Advance Shipment Notification (ASN) issued and Consignment in transit;

(iii) Delivered – Consignment delivered to Delivery Location;

(iv) Rejected – the Party has rejected all of the Consignment;

(v) Partially Delivered – partial Consignment acceptance by the Party;

(vi) Accepted – the Party has accepted delivery of all Communications Hubs in the Consignment; or

(vii) Cancelled – The Party has cancelled delivery of the Consignment.

5. DELIVERY DOCUMENTATION AND PACKAGING

Pre-handover delivery documentation

5.1 At least two Working Days prior to the Delivery Date for a Consignment, the DCC shall:

(a) notify the relevant Party via email that an ASN for that Consignment is available via the OMS; and

(b) ensure that the ASN is available for that Party to download from the OMS under all OMS Accounts associated with that Party in a Comma Separated Values (CSV) file format. The DCC shall ensure that the content of this CSV file is such that:

(i) the first row contains the column headings for each data item;

(ii) the first column in each subsequent row contains the unique CHF Identifier for a Communications Hub, with all other data items in that row being associated to that CHF Identifier;

(iii) the column headings contain the information listed under the header Advanced Shipment Notification in Annex A of this document for the relevant Region;

(iv) fields shall be comma-separated;

(v) fields shall only contain ASCII characters;

(vi) text fields shall be enclosed with opening and closing double quotation marks, but no quotation marks shall be used in date and numeric fields;

(vii) a (double) quote character within a text field must be represented by two (double) quote characters;

(viii) blank fields shall not contain characters other than opening and closing double quotation marks for text fields; and

(ix) records shall be terminated with a line feed (ASCII 10) character.

Delivery documentation and labelling

5.2 The DCC shall ensure that in relation to each Consignment, each carton and pallet will be labelled with identification information as listed under the columns titled “Carton Labels” and “Pallet Labels” in Annex A of this document.

5.3 The DCC shall ensure that a hard copy of the Delivery Note is provided to the Party on the arrival of the Consignment at the Delivery Location.

Communications Hub packaging and labelling information

5.4 The DCC shall permanently mark the identification information listed under the header CH Marking in Annex A of this document onto the front face of each Communications Hub, where that front face is the face of the Communications Hub which contains the M4 retaining screw.

Carton Packaging

5.5 The DCC shall provide packaged Communications Hubs in cardboard boxes within cartons, each carton containing the quantities of Communications Hubs for the relevant Region as set out in Annex B of this document.

5.6 The DCC shall provide cartons that contain only a single Communications Hub Variant.

Pallet Sizes

5.7 The DCC shall ensure that:

(a) cartons are loaded onto pallets of the relevant dimensions for a Region as set out in Annex B of this document;

(b) pallets are wrapped such that cartons are safely secured for transit, and that pallet and carton labelling is visible through the wrapping materials; and

(c) pallets are packed so as not to exceed the maximum specifications as set out in Annex B of this document.

6. HANDOVER PROCEDURE

Pre-delivery Checks

6.1 The DCC shall ensure that, prior to making the ASN for a Consignment available to a Party in accordance with clause 5.1(b), such ASN correctly identifies the total quantity of Communications Hub Device Models requested in that Consignment.

6.2 Each Party (other than the DCC) shall validate the content of an ASN provided to it against the relevant Consignment details derived from its submitted Communications Hub Order to check that the ASN correctly identifies the total quantity of Communications Hub Device Models requested in that Consignment by that Party.

6.3 Where a Party identifies that the ASN is incorrect, it shall notify the DCC using contact details provided in accordance with clause 3.16. The Party shall ensure that this notification is sent to the DCC at least 5 Working Hours before the Delivery Window for that Consignment.

6.4 Where the DCC receives a notification in accordance with clause 6.3, and where DCC agrees that the ASN does not reflect the Consignment, the DCC shall amend the ASN to correctly reflect the requested Consignment promptly and may propose amendments to the Delivery Date. The DCC shall notify the Party via email and via telephone of the steps that it has taken.

Delivery Changes

6.5 Where, prior to the Delivery Date, the DCC becomes aware that it will be unable to deliver the Consignment on the specified Delivery Date, it shall notify the affected Party of the delay and explain the reasons for the delay as soon as reasonably practicable via email and telephone and shall propose amendments to the Delivery Date.

6.6 Where DCC seeks to change a Delivery Date and Delivery Window in accordance with clause 6.4 or 6.5 the DCC shall list reasonable potential options for revised Delivery Dates and Delivery Windows and request a revised Delivery Date and Delivery Window from the affected Party.

6.7 Where a Party is notified in accordance with clause 6.6, the Party shall indicate which one of the potential Delivery Dates and Delivery Windows it prefers, and the DCC shall update the OMS with the Party's preferred rescheduled Delivery Date and Delivery Window for the affected Consignment.

6.8 Where, on or prior to the Delivery Date, the DCC considers that the Consignment will be delivered outside of the Delivery Window, the DCC shall notify the Party as soon as reasonably practicable via notification email and telephone. The DCC shall explain the reason for the delay and provide an estimate for a revised delivery time.

6.9 Where the Party is not able to accept the Consignment at the revised delivery time proposed pursuant to clause 6.8, the DCC shall provide a list of reasonable potential options for revised Delivery Dates and Delivery Windows and request a revised Delivery Date and Delivery Window from the Party. The Party shall indicate which one of the potential Delivery Dates and Delivery Windows offered by the DCC it prefers, and the DCC shall update the OMS accordingly.

Unloading

6.10 On the Delivery Date the Party shall:

(a) ensure that there is access for the DCC to the Delivery Location during the Delivery Window; and

(b) provide a dry receiving area large enough to receive all the pallets in the Consignment.

6.11 When the Consignment arrives at a Party's Delivery Location that Party shall:

(a) check the Delivery Note information to confirm that the Consignment matches the relevant ASN prior to unloading;

(b) protect the Consignment from moisture and extremes of temperature during unloading in accordance with the environmental conditions set out in Annex C of this document, and as amended from time to time;

(c) except where not required to do so pursuant to clause 6.12, unload pallets from the delivery vehicle; and

(d) unload the vehicle within two hours of the later of:

(i) the agreed Delivery Window: or

(ii) the delayed delivery arrival time where the delivery is delayed.

6.12 A Party:

(a) shall not unload pallets that are not identified on the ASN;

(b) may decline to unload pallets where pursuant to clause 6.18 they are going to reject a complete pallet; and

(c) may decline to unload pallets where to do so would present a health and safety risk.

6.13 Any pallets that are not unloaded for the reasons set out in clause 6.12 of this document shall be deemed to be rejected by the relevant Party, and that Party shall provide a notification to the DCC in accordance with clause 6.20 of this document.

Consignment Reconciliation

6.14 Following unloading, and without removing any packaging or breaking any security seals on the delivered pallets or Communications Hubs, the Party shall take reasonable steps to:

(a) scan or visually inspect the label on each unloaded pallet, and confirm that the

(i) pallet identifier;

(ii) OMS Order Reference;

(iii) Consignment reference; and

(iv) any carton identifiers that are visible,

match those shown on the ASN; and

(b) verify that the quantity of cartons on each pallet matches the quantity shown on the ASN.

6.15 The Party shall sign the Delivery Note to confirm completion of delivery prior to the delivery vehicle departing the Delivery Location.

6.16 If the Party is aware of any discrepancies that exist between the pallets or cartons of Communications Hubs unloaded and the information contained within the ASN or the Delivery Note, the Party shall note this on the Delivery Note prior to signing it.

6.17 The DCC shall ensure that the Party is provided with a hard copy of the signed Delivery Note as proof of delivery prior to the delivery vehicle leaving the Delivery Location.

Visual Inspection

6.18 In addition to the right to reject pursuant to Section F6.9 (a) to (c), a Party shall reject a complete pallet where any of the following is identified:

(a) heat or smoke damage to the external wrapping or packaging;

(b) evidence of tampering or interference with any packaging tamper seals; or

(c) damage, which is estimated to affect more than 50% of the cartons on that pallet as a result of:

(i) fork lift truck/handling damage or outer-wrapping damage where there are notable signs of packaging or product damage such as crushing, puncturing or scraping;

(ii) water ingress, or other liquid or chemical damage; or

(iii) signs of infestation by pests or mould.

6.19 Pursuant to Section F6.9 (d), a Party receiving a Consignment may reject individual damaged cartons where it has not rejected the whole pallet as set out in clause 6.18.

Delivery Confirmation Procedure

6.20 Pursuant to Section F6.7, a Party shall provide confirmation of whether or not a delivery of Communications Hubs Products has been made in compliance with the order by notifying the DCC via the OMS using either the CH Ordering or the CH Delivery and Returns profile. Such notification shall include details of any pallets or where applicable, individual cartons of Communications Hubs that are rejected, and provide the following:

(a) OMS Order Reference;

(b) Consignment reference;

(c) where a complete pallet is rejected:

(i) the pallet identifier;

(ii) quantity of cartons on the pallet; and

(iii) a description of the reason for rejection as listed in clause 6.21; and

(d) where a carton is rejected that is not part of a complete pallet:

(i) carton identifier; and

(ii) a description of the reason for rejection as listed in clause 6.21.

6.21 For the purposes of the notification under clause 6.20, the reason for rejection of all or part of a Consignment is one of those listed in Section F6.9 (a) to (c), or one of the following:

(a) pallet not unloaded for the reasons set out in clause 6.12;

(b) pallet rejected in accordance with clause 6.13;

(c) missing pallet from the Consignment as unloaded;

(d) pallet not identified within the Party’s ASN for that Consignment;

(e) pallet rejected in accordance with clause 6.18;

(f) carton missing from the Consignment as unloaded;

(g) carton not identified within the Party’s ASN for that Consignment; or

(h) carton rejected in accordance with clause 6.19.

6.22 A Party may only reject whole cartons of Communications Hubs.

Rejected Delivery Return Procedure

6.23 Following the receipt of a notification via the OMS in accordance with clause 6.20 of this document, the DCC shall notify the Party via an email to all OMS Accounts associated with that Party, that a Delivery Issues Report Notification (DIRN) for rejected Communications Hubs is available via the OMS, or include the DIRN within the email notification, within one Working Day. The DIRN shall contain the following:

(a) a unique DIRN reference;

(b) the date and time for collecting the Communications Hubs to be returned which shall be within five Working Days of the receipt of the notification.

6.24 Where the Party is unable to accommodate the collection date and time specified in the DIRN, it shall notify the DCC within one Working Day of receipt of the notification in accordance with clause 6.23 using the contact details published via the OMS for this purpose, and the DCC shall list reasonable potential options for revised collection dates and times and request a revised collection date and time from the Party, and that Party shall notify the DCC using the contact details published via the OMS for this purpose of its preferred collection date and time from the options presented.

6.25 The DCC make a printable DIRN label available via the CH Ordering System for each unique DIRN reference within one Working Day of either:

(a) the receipt of the notification of rejection in accordance with clause 6.20; or

(b) notification by the Party of its preferred collection date and time in accordance with clause 6.24.

6.26 Parties shall ensure that rejected Communications Hubs are packaged in the cartons in which they were originally received and loaded so as not to exceed the maximum number of Communications Hubs per layer and layers per pallet as set out in Annex B of this document. The Party shall print and securely attach the DIRN label to the outside of each complete pallet or where the pallet is not complete on the outside of each carton that is to be returned.

Rejected Delivery Return Handover Procedure

6.27 When the collection vehicle arrives at a Party's Delivery Location, that Party shall:

(a) load the vehicle within two hours of the collection time; or

(b) load the vehicle within two hours of the time that the collection vehicle arrives at the Delivery Location, where the delivery vehicle arrives within two hours of the collection time and the arrival time is during Working Hours and where the Party can reasonably be expected to have completed loading during Working Hours;

(c) take reasonable steps to load the vehicle within two hours where the arrival time is later than two hours of the collection time and the arrival time is during Working Hours and where the Party can reasonably be expected to have completed loading during Working Hours;

(d) during loading, protect the goods from moisture and extremes of temperature in accordance with the environmental conditions set out in Annex C of this document, and as amended from time to time; and

(e) only load pallets or cartons with IDs that are included on the DIRN and that have a valid DIRN label attached onto the collection vehicle.

6.28 Where it is not possible to fulfil the collection and the DCC (or a Party) seeks to rearrange a collection date and collection window, the DCC shall list reasonable potential options for revised collection dates and collection windows and request a revised collection date and collection window from the affected Party. The Party shall choose a revised date and time from the options provided.

6.29 Where requested to do so the DCC shall sign the Party's collection note to confirm completion of collection prior to the collection vehicle departing the Delivery Location and the Party may provide a hard copy of the collection note to the DCC prior to the collection vehicle leaving the Delivery Location.

Delivery of Replacement Communications Hubs

6.30 Pursuant to Section F6.13, where a Party notifies the DCC of rejection for non- compliance of all or part of a Consignment in accordance with clause 6.20 of this document, the DCC shall by the next Working Day provide to the Party a list of reasonable potential options for revised Delivery Dates and Delivery Windows in respect of replacement goods and request a revised Delivery Date and Delivery Window from the Party. The Party shall indicate which one of the potential Delivery Dates and Delivery Windows offered by the DCC it prefers, and the DCC shall update the OMS accordingly.

6.31 Following the receipt of the DCC notification in accordance with clause 6.30, the replacement goods shall be treated as if a Consignment being delivered as part of a Valid Communications Hub Order and Sections 5 and 6 of this document shall apply accordingly.

7. HANDOVER PROCEDURE – SPECIAL INSTALLATION MESH COMMUNICATIONS HUBS (SOUTH REGION AND CENTRAL REGION)

7.1 Where the DCC is in attendance at a premises in accordance with the special installations and modifications procedure as described in the CH Installation and Maintenance Support Materials, the DCC shall, subject to Section F7.4A(b), provide the Party with such Special Installation Mesh Communications Hubs as are required to complete the installation.

7.2 The DCC shall provide Special Installation Mesh Communications Hubs in individual packaging as described in Annex D of this document.

7.3 On receipt of a Special Installation Mesh Communications Hub, the Party shall undertake a visual inspection of the device packaging. In addition to the right to reject pursuant to Section F7.4A, a Party shall reject a Special Installation Mesh Communications Hub where any of the following is identified:

(a) heat or smoke damage to the external packaging;

(b) evidence of tampering or interference with any packaging tamper seals; or

(c) other damage, which may be reasonably identified as a result of:

(i) handling damage or outer-wrapping damage where there are notable signs of packaging or product damage such as crushing, puncturing or scraping;

(ii) water ingress, or other liquid or chemical damage; or

(iii) signs of infestation by pests or mould.

7.4 The DCC shall also make available any aerial that it plans to install with the Special Installation Mesh Communications Hub for inspection by the Party. This shall include any of the following variants (T1 Aerial Type, T2 Aerial Type, T3 Aerial Type, M1 Aerial Type and M2 Aerial Type) as deemed necessary.

7.5 The completion of hand over of the Special Installation Mesh Communications Hub for the purposes of Section F7.4A (c), shall be deemed to have occurred following the inspection and acceptance of the Special Installation Mesh Communications Hub by the Party.

7.6 In the event that a Special Installation Mesh Communications Hub is rejected and the DCC is in attendance and where the Party wishes to hand back the Special Installation Mesh Communications Hub the DCC shall accept the rejected Special Installation Mesh Communications Hub and shall provide a replacement immediately, subject to Section F7.4A(b). In the event that the Supplier considers that any of the aerials provided by the DCC is damaged and requests a replacement, the DCC shall make available a replacement for inspection.

8. COMMUNICATIONS HUB STORAGE AND TRANSIT REQUIREMENTS

Storage Conditions

8.1 Parties shall ensure that whilst the Party is in possession of the Communications Hub, Communications Hubs shall be handled, stored and delivered in accordance with the environmental conditions detailed in Annex C of this document.

Transit to and from Consumer Premises

8.2 Parties shall ensure that when transporting Communications Hubs, they meet the specifications as described in Annex D.1.1 and D.1.2 of this document.

8.3 Parties shall take reasonable steps to install Communications Hubs from stock on a ‘first-in-first out’ basis such that Communications Hubs are not held in storage for longer than is necessary.

9. COMMUNICATIONS HUB TRANSFER

Communications Hub Transfer Request

9.1 Following receipt of a Communications Hub Transfer Request in accordance with Section F6A, the DCC shall notify via email the following information:

(a) a unique reference for the Communication Hub Transfer Request

(b) the associated date which shall be where a Communications Hub Transfer Request has been submitted by a Party, the date of submission.

9.2 Where a Party notifies the DCC of Communications Hubs available to transfer in accordance with Section F6A.4, the Party shall:

(a) verify that the SMI Status of the Communications Hubs is ‘pending’;

(b) specify the CHF Identifier (EUI-64 unique number) for each available Communications Hub;

(c) provide the following information for each Transfer Location:

(i) the full delivery address;

(ii) operating hours; and

(iii) the name, email address, and telephone number for a nominated contact in relation to Communications Hub Transfers.

Transfer Dates and Time Amendments

9.3 Following acceptance of a Communications Hub Transfer Request, the transferring Party shall specify a Transfer Window. Such Transfer Window shall be submitted to the DCC via email.

9.4 Following acceptance of a Communications Hub Transfer Request, either of the requesting Party or the transferring Party may request amendments to the Transfer Date or Transfer Window up to 30 days prior to the original Transfer Date. Such requests shall be submitted to the DCC via email.

9.5 Any request by a Party for an amendment pursuant to clause 9.4, is subject to the following restrictions:

(a) the revised Transfer Date must be a Working Day within five days of the original Transfer Date; and

(b) the revised Transfer Window must be within Working Hours.

9.6 Following receipt of a notice or request under Clause 9.4 or 9.5, the DCC shall notify the other Party via email and that Party shall respond by emailing indicating (at its discretion) whether the Transfer Date or Transfer Window is:

(a) accepted;

(b) rejected; or

(c) rejected subject to a counterproposal.

9.7 The DCC shall confirm acceptance, rejection or rejection and counterproposal to the other Party as soon as reasonably practical and in any event within five Working Days of the request having been made.

9.8 Where pursuant to clause 9.6 the DCC confirms to a Party that a change to the Transfer Date or Transfer Window is accepted, the requesting Party shall be obliged to collect the Communications Hub Transfer in accordance with those updated instructions.

Transfer Documentation and Packaging

9.9 At least two Working Days prior to the Transfer Date, the DCC shall:

(a) notify the relevant Parties via email that an ASN for that Communications Hub Transfer is available for download via the DCC SharePoint; and

(b) ensure that the ASN is available for both transferring Parties to download from SharePoint in a Comma Separated Values (CSV) file format.

9.10 The DCC shall ensure that the content of this CSV file is such that:

(a) the first row contains the column headings for each data item;

(b) the first column in each subsequent row contains the unique CHF Identifier for a Communications Hub, with all other data items in that row being associated to that CHF Identifier;

(c) the column headings contain the information listed under the header Advanced Shipment Notification in Annex A of this document for the relevant Region;

(d) fields shall be comma-separated;

(e) fields shall only contain ASCII characters;

(f) text fields shall be enclosed with opening and closing double quotation marks, but no quotation marks shall be used in date and numeric fields;

(g) a (double) quote character within a text field must be represented by two (double) quote characters;

(h) blank fields shall not contain characters other than opening and closing double quotation marks for text fields; and

(i) records shall be terminated with a line feed (ASCII 10) character.

9.11 The DCC shall provide printable labels via SharePoint at least two Working Days prior to the Transfer Date to the Party transferring Communications Hubs to allow the Party to label each carton and pallet with identification information as listed under the columns titles “Carton Labels” and “Pallet Labels” in Annex A of this document.

9.12 The Party transferring Communications Hubs shall ensure a hard copy of the Transfer Note is provided to the requesting Party on collection of the Communications Hubs from the Transfer Location.

9.13 The Party transferring Communications Hubs shall ensure that all Communications Hub transferred are in packaging of equivalent standard to that in which a Communications Hub of that Device Model was originally packaged, not exceeding the maximum number of Communications Hubs per carton and cartons per pallet set out in Annex B of this document.

9.14 The Party transferring Communications Hubs shall ensure that:

(a) cartons are loaded onto pallets of the relevant dimensions for a Region as set out in Annex B of this document;

(b) pallets are wrapped such that cartons are safely secured for transit, and that pallet and carton labelling is visible through the wrapping materials; and

(c) pallets are packed so as not to exceed the maximum specifications as set out in Annex B of this document.

Pre-transfer Checks

9.15 The DCC shall ensure that, prior to making the ASN for a Communications Hub Transfer available to the requesting Party in accordance with clause 9.9(b), such ASN correctly identifies the total quantity of Communications Hub Device Models requested.

9.16 Each of the requesting Party and the transferring Party shall validate the content of an ASN provided against the relevant Communications Hub Transfer details derived from its submitted Communications Hub Transfer Request to check the ASN correctly identifies the total quantity of Communications Hub Device Models requested.

9.17 Where a Party identifies that the ASN is incorrect, it shall notify the DCC using the contact details provided in accordance with clause 9.2. The Party shall ensure that this notification is sent to the DCC at least 5 Working Hours before the Transfer Window for that transfer.

9.18 Where the DCC receives a notification in accordance with clause 9.17 and where the DCC agrees that the ASN does not reflect the Communications Hub Transfer, the DCC shall amend the ASN to correctly reflect the requested Communications Hub Transfer and may propose amendments to the Transfer Date. The DCC shall notify the Party via email and via telephone of the steps that it has taken.

Transfer Changes

9.19 Where, prior to the Transfer Date, a requesting Party becomes aware that it will be unable to collect the Communications Hubs on the specified Transfer Date, it shall notify the DCC of the delay and explain the reasons for the delay as soon as reasonably practicable via email and via telephone and shall propose amendments to the Transfer Date.

9.20 Where a Party seeks to change a Transfer Date in accordance with clause 9.19 the Party shall list reasonable potential options for revised Transfer Dates and request a revised Transfer Date from the DCC.

9.21 Upon receipt of a notification in accordance with clause 9.19 and 9.20, the DCC shall notify the transferring Party providing the list of potential options for revised Transfer Dates.

9.22 Where the transferring Party is notified in accordance with clause 9.21, the Party shall indicate which one of the potential Transfer Dates it prefers, and the DCC shall update all affected Parties with the preferred rescheduled Transfer Date via email.

9.23 Where, on or prior to the Transfer Date, a Party considers that the Communications Hub Transfer will be collected outside of the Transfer Window, the Party shall notify the DCC as soon as reasonably practicable via notification email and telephone. The Party shall explain the reason for the delay and provide an estimate for a revised delivery time.

9.24 Upon receipt of a notification in accordance with clause 9.23, the DCC shall notify the affected Party providing all notified information.

9.25 Where the affected Party is not able to accept the Communications Hub Transfer at the revised transfer time proposed pursuant to 9.23, the DCC shall provide a list of reasonable potential options for revised Transfer Dates and Transfer Windows and request a revised Transfer Date and Transfer Window from the Party. The Party shall indicate which one of the potential Transfer Dates and Transfer Windows offered it prefers, and the DCC shall update all affected Parties via email accordingly.

Loading of Transfer

9.26 On the Transfer Date the transferring Party shall:

(a) ensure that there is access for the requesting Party to the Transfer Location during the Transfer Window; and

(b) provide a dry receiving area large enough to load all the pallets in the Communications Hub Transfer.

9.27 When the requesting Party arrives at a Party's Transfer Location that Party shall:

(a) check the Transfer Note information to confirm that the Communications Hub Transfer matches the relevant ASN prior to loading;

(b) undertake a visual inspection of the Communications Hubs in accordance with clause 9.34;

(c) protect the Communications Hubs from moisture and extremes of temperature during loading in accordance with the environmental conditions set out in Annex C of this document, and as amended from time to time;

(d) except where not required to do so pursuant to clause 9.28, load pallets from the Transfer Location; and

(e) load the vehicle:

(i) within the agreed Transfer Window: or

(ii) within two hours of the delayed transfer arrival time where the transfer is delayed and notified under clause 9.22.

9.28 A requesting Party:

(a) shall not load pallets that are not identified on the ASN;

(b) shall decline to load pallets where pursuant to clause 9.34 they are going to reject a complete pallet; and

(c) shall decline to load pallets where to do so would present a health and safety risk.

9.29 Any pallets that are not loaded for the reasons set out in clause 9.28 of this document shall be deemed to be rejected by the relevant Party, and that Party shall provide a notification to the DCC in accordance with clause 9.36 of this document.

Transfer Reconciliation

9.30 Following loading, and without removing any packaging or breaking any security seals on the collected pallets or Communications Hubs, the requesting Party shall take reasonable steps to:

(a) scan or visually inspect the label on each loaded pallet, and confirm that the

(i) pallet identifier;

(ii) Communications Hub Transfer reference; and

(iii) any carton identifiers that are visible,

match those shown on the ASN; and

(b) verify that the quantity of cartons on each pallet matches the quantity shown on the ASN.

9.31 Each Party shall sign the Transfer Note to confirm completion of collection prior to the collection vehicle departing the Transfer Location.

9.32 If a Party is aware of any discrepancies that exist between the pallets or cartons of Communications Hubs loaded and the information contained within the ASN or the Transfer Note, the Party shall note this on the Transfer Note prior to signing it.

9.33 The transferring Party shall ensure that the requesting Party is provided with a hard copy of the signed Transfer Note as proof of collection prior to the collection vehicle leaving the Transfer Location.

Transfer Visual Inspection

9.34 In addition to the right to reject pursuant to Section F6A.15, a Party shall reject a complete pallet where any of the following is identified:

(a) heat or smoke damage to the external wrapping or packaging;

(b) evidence of tampering or interference with any packaging tamper seals; or

(c) damage, which is estimated to affect more than 50% of the cartons on that pallet as a result of:

(i) fork lift truck/handling damage or outer-wrapping damage where there are notable signs of packaging or product damage such as crushing, puncturing or scraping;

(ii) water ingress, or other liquid or chemical damage; or

(iii) signs of infestation by pests or mould.

9.35 The requesting Party may reject individual damaged cartons where it has not rejected the whole pallet as set out in clause 9.34.

Transfer Confirmation Procedure

9.36 Pursuant to Section F6A.13, a Party shall provide confirmation of whether or not a transfer of Communications Hubs has been made in compliance with the request by notifying the DCC via email. Such notification shall include details of any pallets or where applicable, individual cartons of Communications Hubs that are rejected, and provide the following:

(a) Communication Hub Transfer Request Reference;

(b) where a complete pallet is rejected:

(i) the pallet identifier;

(ii) quantity of cartons on the pallet; and

(iii) a description of the reason for rejection as listed in clause 9.37; and

(c) where a carton is rejected that is not part of a complete pallet:

(i) carton identifier; and

(ii) a description of the reason for rejection as listed in clause 9.37.

9.37 For the purposes of the notification under clause 9.36, the reason for rejection of all or part of a Communications Hub Transfer is one of those listed in Section F6A.15, or one of the following:

(a) pallet not loaded for the reasons set out in clause 9.28;

(b) pallet rejected in accordance with clause 9.29;

(c) missing pallet from the Communications Hub Transfer as loaded;

(d) pallet not identified within the Party's ASN for that Communications Hub Transfer;

(e) pallet rejected in accordance with clause 9.34;

(f) carton missing from the Communications Hub Transfer as loaded;

(g) carton not identified within the Party's ASN for that Communication Hub Transfer; or

(h) carton rejected in accordance with clause 9.35.

9.38 A Party may only reject whole cartons of Communications Hubs.

Annex A. Consignment Information

A.1. Consignment labelling and information

A.1.1 Table 1 below describes the information provided for each Communications Hub, each carton containing a Communications Hub and each pallet of Communications Hubs for delivery, depending upon the Region to which the associated Communications Hub Order relates. A summary of data items included in the Advance Shipment Notification and the associated Delivery Note is also provided.

Table 1; Consignment labelling and information

	CH Marking		Carton Labels	Pallet Labels	Advanced Shipment Notification		Delivery/Transfer Note	
	North Region	Central & South Regions	All Regions	All Regions	North Region	Central & South Regions	North Region	Central & South Regions
CHF Identifier (EUI-64 unique number)	Y	Y	Y		Y	Y		
Communications Hub Variant	Y	Y	Y	Y	Y	Y	Y	Y
GPF identifier (EUI-64 unique number)	Y	Y			Y	Y		
Zigbee MAC address	Y	Y			Y	Y		
SM WAN identifier					Y			

OMS Order Reference				Y	Y	Y	Y	Y
Party order reference				Y	Y	Y	Y	Y
Consignment reference				Y	Y	Y	Y	Y
Delivery Location					Y	Y	Y	Y
Scheduled Delivery Date and Time					Y	Y	Y	Y
Firmware version number					Y	Y		
Hardware version number	Y				Y	Y		
Device configuration identifier	Y				Y			
Manufacturer, country and date of manufacture	Y	Y			Y	Y		
Batch number					Y	Y		
Reconditioned status (Y/N)					Y	Y		
Pallet identifier				Y	Y	Y	Y	Y
Quantity of Cartons on the pallet				Y	Y	Y	Y	Y
Carton identifier			Y	Y	Y	Y	Y	Y
Quantity of Communications Hubs in carton			Y		Y	Y	Y	Y
Pallets in delivery					Y	Y	Y	Y

Annex B. Communications Hub Pallet and Carton Quantities

B.1. Communications Hub Packaging

B.1.1 Consignments will be delivered in accordance with the packaging quantities set out in Table 2 below. Maximum delivery volumes assume double stacked pallets. Individual Communications Hub Consignments may therefore include pallets in different pallet layers.

B.1.2 Where Communications Hub Orders in the North Region are placed for multiple Communications Hub Variants, these Communications Hub Variants will be delivered on separate pallets. Pallets will not contain a mix of different Communications Hub Variants.

Table 2; Communications Hub delivery packaging

Packaging Information	North Region	Central Region and South Region
DCC Pallet size	Standard 4 Way L:1.2m, w:1m, H: 1m	Standard 4 Way L:1.2m, w:1m, H: 1m
Packaged Communications Hubs per carton	28	Either: 14 – Single Band Cellular Communications Hub Variant or 10 – all Communications Hub Variants except the Single Band Cellular

		Communications Hub Variant
Cartons per layer	8	16
Maximum layers per pallet	4	4
Cartons per full pallet	32	64
Boxes per full pallet	896 (28 boxes x 32 cartons)	Between 640 and 896 (64 cartons, each containing either 10 or 14 boxes)
Actual weight per full pallet	333 kg for Single Band Communications Hubs 200 kg for Dual Band Communications Hubs - Standard 420 DB Variant (est.)	
Maximum weight per pallet		Max 500 kg
Maximum pallet height (incl. Pallet base)	1m	1m
Maximum volume (m3) per pallet	1.2 m3	1.2 m3
Maximum Pallets per trailer	52	40
Maximum packaged Communications Hubs per trailer	46,592	Between 25,600 and 35,840

Annex C. Communications Hub storage and installation environmental conditions

C.1. Storage and installation environmental conditions

C.1.1 Communications Hubs are designed to be stored and operated within a defined range of environmental conditions; exposure to conditions outside this range may lead to premature failure of the device.

C.1.2 Communications Hubs are designed to be stored under the following conditions:

(a) individual Communications Hubs should be kept in the original packaging provided for shipment prior to installation;

(b) any storage environment should meet European Telecoms Standards Institute ETSI EN 300 019-1-.1 Class 1.2 (Weather protected not temperature- controlled storage locations), or any equivalent standard that replaces this; and

(c) Good Industry Practices suitable for the handling, storage, preservation and internal delivery of the inventory of Communications Hubs that prevent damage, deterioration or misuse during internal processing should be followed.

C.1.3 Communications Hubs are designed to be transported in the following conditions:

(a) individual Communications Hubs should be transferred between locations packaged in their original packaging such that they are protected from damage during normal handling; and

(b) the transport environment should meet the European Telecoms Standards Institute ETSI EN 300 019-1-.2 Class 2.3 (Public Transportation), or any equivalent standard that replaces this.

C.1.4 Communications Hubs are designed to be installed and operated under the following conditions:

(a) the Communications Hub should not be subject to moisture ingress or foreign object ingress during the installation process;

(b) following correct installation onto an ICHS-compliant host, moisture or foreign object ingress conditions should not exceed that specified in the IP53 Code under IEC standard 60529 or any equivalent standard that replaces this;

(c) the Communications Hub should not be subject to humidity outside the range of 10% to 90% non-condensing; and

(d) the Communications Hub should not be exposed to extremes of temperature of below -20°C or above +55°C.

Annex D. Communications Hub Packaging

D.1.1. Communications Hubs will be individually packaged in a cardboard box that:

(a) is robust enough to protect the ICHIS connector pins during transport and handling; and

(b) allows for both the CHF Identifier and Communications Hub Variant information to be visible directly through a cut-out without removing any of the packaging.

D.1.2. Individually boxed Communications Hubs will be grouped and packed in cardboard cartons that:

(a) protect the Communications Hub from damage during transport and handling;

(b) will contain the quantities set out in Annex B;

(c) are labelled in accordance with Annex A; and

(d) contain a single Communications Hub Variant.

D.1.3. Cartons of Communication Hub will be delivered on UK standard pallets in the quantities per pallet set out in Annex B. The pallets will be wrapped in industrial pallet or stretch wrap material.

Version I 5.0

APPENDIX I

CH Installation and Maintenance Support Materials

Definitions

Cellular Communications	means a WAN Variant in the Central Region and the South Region which is capable of using mobile cellular radio technology to connect to the SM WAN.
Central Region	means the Region which covers the majority of Wales and the majority of central England.
CH No SM WAN Installation Procedure	means the procedure by which a Supplier Party installs a Communications Hub where it has not established a connection to the SM WAN as described in clauses 4.8 to 4.10 of this document
CH Status Information	means the visual information that is displayed by the Communications Hub to indicate the current operational status of the Communications Hub, as further set out in the CH Supporting Information.
CH Supporting Information	has the meaning given to that term in the CH Handover Support Materials.
CHF Identifier	has the meaning given to that term in CHTS.
Communications Hub Availability and Diagnostics Check	means the procedure set out in clause 5.2 of this document.
Communications Hub Fault Handling Procedures	means the processes set out in clauses 8.3 to 8.11 of this document.
Communications Hub Variants	means variations of Communications Hubs describing their HAN and WAN communications characteristics.
Coverage Area	means the geographical coverage of the SM WAN at a point in time.
DCC Installer Training Plan	means the training materials provided by the DCC to support the development of Communications Hub installation and maintenance training.
DCC Returns Location	means a location at which a Party should deliver Communications Hubs that it wishes to return to the DCC.
Dual Band Communications Hub	a HAN Variant which is capable of using 2.4GHz and Sub-GHz frequencies for communication on the Home Area Network (HAN).
Fault Analysis Report	means the report provided to a Party by the DCC pursuant to Section F9.11 of the Code.

Installation Location	means the location of a premises at which a Communications Hub is planned to be, or has been, installed.
Installation Point	means the location at an Installation Location where a Communications Hub is installed.
Mesh Communications Hub	means a WAN Variant in the Central Region and the South Region which is capable of using both mobile cellular radio technology and wireless mesh radio technology to connect to the SM WAN.
North Region	means the Region which covers the majority of Scotland and the majority of northern England.
Order Management System (or **OMS)**	has the meaning given to that term in the CH Handover Support Materials.
Return Date	means the date on which a Communications Hub is arranged to be delivered to the DCC by a Party
Return Delivery Note	means an electronic or paper form containing the information set out in clause 10.12.
Return Materials Authorisation (or **RMA**)	means the procedure whereby the DCC authorises a Party's request to return a Communications Hub to the DCC in accordance with clauses 10.5 to 10.7 of this document.
Significant Metallic Obstruction	means a metallic object of such scale and proximity to the Communications Hub as is likely to cause obstruction to SM WAN communications to the Communications Hub, and as further described in the CH Supporting Information.
Single Band Communications Hub	means a HAN Variant which is only capable of using 2.4GHz frequency for communication on the Home Area Network (HAN).
Special Installation Mesh Communications Hub	means a WAN Variant in the Central Region and the South Region which provides two external aerial ports on the front face to enable connection of two external aerials – one cellular (either a T1 Aerial Type, T2 Aerial Type or T3 Aerial Type) and one mesh (either an M1 Aerial Type or M2 Aerial Type). This WAN variant may not be ordered by Parties but is supplied and fitted directly by DCC.
South Region	means the Region which covers the majority of southern England.
Substantial Stone Walls	means walls with external or internal structure primarily made of stone, and of sufficient thickness to be likely to prevent connectivity to the SM WAN by the Communications Hub, as further described in the CH Supporting Information.

Working Hours	has the meaning given to that term in the CH Handover Support Materials.

1. INTRODUCTION

Document purpose

1.1 Sections F7 to F9 set out principal rights and obligations applying to the installation and maintenance of Communications Hubs, which are supplemented by the provisions set out below. This document forms Appendix I of the Code.

General clarifications

1.2 Unless expressly stated otherwise, the obligations set out in this document are applicable to all Regions.

1.3 Unless expressly stated otherwise none of the obligations in this document apply to Test Communications Hubs.

2. GENERAL OBLIGATIONS IN RELATION TO THE INSTALLATION AND MAINTENANCE OF COMMUNICATIONS HUBS

DCC Obligations

2.1 The DCC shall ensure that it provides upon request to Parties a DCC Installer Training Plan which is sufficient to enable individuals accredited in accordance with it to carry out Communications Hub installation and maintenance activities in accordance with the CH Support Materials.

Supplier Party Obligations

2.2 Each Supplier Party shall ensure that any installations or maintenance of Communications Hubs undertaken on its behalf are undertaken by individuals that are certified to carry out Communications Hub installation and maintenance activities in accordance with the process for independent certification set out in the DCC Installer Training Plan.

3. PRE-INSTALLATION PROCEDURES

Activation prior to installation

3.1 A Party shall take all reasonable steps to prevent any Communications Hub in its possession from establishing a connection to the SM WAN prior to its installation for the purposes of Commissioning the Communications Hub Function.

Communications Hub inspections prior to installation

3.2 When installing a Communications Hub, prior to removing any packaging, a Supplier Party shall ensure that visual checks are undertaken to confirm that the packaged Communications Hub is not damaged.

3.3 Following the removal of all packaging, a Supplier Party shall ensure that visual checks are undertaken to confirm that the connecting pins (as described in the ICHIS) on the Communications Hub appear to be aligned and that the Communications Hub is not otherwise visibly damaged.

3.4 Where a Party, following inspection in accordance with clauses 3.2 and 3.3 above identifies damage to the Communications Hub or its packaging (including where the connecting pins are misaligned) that has caused or may reasonably be assumed to have caused more than superficial scratching or cosmetic damage to the body of the Communications Hub, the Party shall not attempt to install the Communications Hub and shall return the Communications Hub in accordance with clauses 10.1 to 10.20 of this document.

Pre-requisites for Fitting of Communications Hubs

3.5 Each installing Supplier Party shall ensure that a Communications Hub is not installed where it ascertains that:

(a) the environmental conditions as defined in Annex C of the CH Handover Support Materials are not met; or

(b) the estimated temperature difference between the Communications Hub to be installed and the ICHIS compliant host exceeds 10 degrees Celsius.

3.6 Prior to attempting a Communications Hub installation, a Supplier Party shall ensure that the Installation Point is visually inspected to assess whether it lies entirely within a metallic enclosure or if any Significant Metallic Obstruction(s) exists. A Supplier Party shall ensure that a Communications Hub is not installed where its visual inspection determines that:

(a) the Installation Point is entirely within a metallic enclosure; or

(b) a Significant Metallic Obstruction exists with respect to three or more of the following surfaces:

(i) the front surface of the Communications Hub;

(ii) the top surface of the Communications Hub;

(iii) the left-side surface of the Communications Hub; or

(iv) the right-side surface of the Communications Hub;

and where (a) or (b) applies that the use of an aerial is not determined to be likely to provide connectivity.

4. COMMUNICATIONS HUB INSTALLATION

4.1 When attempting the initial installation of a Communications Hub, a Supplier Party shall ensure that it uses the WAN Variant that was identified as being required for the Installation Location on the Coverage Database when the Supplier Party checked the Coverage Database, provided that this check was performed at any time within the period 30 days prior to the Installation Date.

4.2 It is a Supplier Party's responsibility to decide which HAN Variant to install at each customer's premises.

4.3 When installing a Communications Hub or Communications Hub Auxiliary Equipment, as set out in the Annex E of this document, a Supplier Party shall ensure that all appropriate tools and equipment are used.

Fitting and activation

4.4 A Supplier Party shall ensure that a Communications Hub is fitted according to the procedure set out in Annex A of this document.

4.5 On completion of the fitting procedure, the relevant Supplier Party shall ensure that the activation procedures for the Device Model that has been fitted are undertaken, as set out in Annex B of this document.

4.6 Where, during the installation process, the Supplier Party suspects that a fault has occurred with the Communications Hub, the relevant Supplier Party shall follow the procedures set out in clauses 8.1 to 8.13 of this document.

Post Installation Update Procedure

4.7 Where following completion of both the relevant fitting procedures and the relevant activation procedures, the Communications Hub is successfully connected to the SM WAN, the relevant Supplier Party shall:

(a) ensure that the Communications Hub is fitted with a security seal; and

(b) submit a Service Request 8.14.1 (Communications Hub Status Update – Installation Success) in accordance with the DUIS within five (5) Working Days.

CH No SM WAN Installation Procedure

4.8 Where, following the fitting and activation procedure, a Supplier Party wishes to leave a Communications Hub installed without establishing a connection to the SM WAN, the Supplier Party shall:

(a) ensure that the power supply to the Communications Hub is capable of being maintained following fitting and activation;

(b) verify that the CH Status Information does not indicate any fault other than failure to connect to the SM WAN;

(c) ensure that the Communications Hub is fitted with a security seal; and

(d) the relevant Supplier Party shall notify the DCC by submitting a Service Request 8.14.2 (Communications Hub Status Update Install No SM WAN) in accordance with the DUIS, within three (3) Working Days.

4.9 Pursuant to 4.8(d) a Supplier Party submitting an 8.14.2 Service Request shall indicate whether each of the following conditions exists:

(a) a Significant Metallic Obstruction exists at the Installation Point with respect to any of the following surfaces;

(i) the front surface of the Communications Hub;

(ii) the top surface of the Communications Hub;

(iii) the left-side surface of the Communications Hub; or

(iv) the right-side surface of the Communications Hub.

(b) (without detailed or expert assessment), the Installation Point appears to have Substantial Stone Walls; or

(c) the Installation Point is in a shared or communal area, outside the individual premises.

4.10 Following receipt of a Service Request 8.14.2 (Communications Hub Status Update Install No SM WAN), the DCC shall create an Incident and shall include within the Incident details of any Network Enhancement Plan affecting the Installation Location.

5. COMMUNICATIONS HUB DIAGNOSTICS

5.1 Where, following successful installation of a Communications Hub and Commissioning of the related Communications Hub Function, a Supplier Party identifies a potential Communications Hub fault, pursuant to Section H9.6 of the Code, that Supplier Party shall take all reasonable steps to complete the Communications Hub Availability and Diagnostics Check procedure prior to raising an Incident with the DCC.

Communications Hub Availability and Diagnostics Check

5.2 A Supplier Party may undertake a Communications Hub Availability and Diagnostics Check, by either:

(a) utilising the Self-Service Interface to complete the Communications Hub availability and diagnostic check as defined in the Self-Service Interface Access Control Specification and the SSI Baseline Requirements Document; or

(b) sending Service Requests 6.13: (Read Event or Security Log) for the CHF event log and Service Request 8.9: (Read Device Log) for the CHF Device Log, in accordance with DUIS and interpreting the Service Responses received.

5.3 Where any Communications Hub Availability and Diagnostics Check indicates that the Communications Hub Function does not:

(a) have a network status of 'activated'; or

(b) the Communications Hub Availability and Diagnostics Check response indicates that an error has occurred;

the Supplier Party shall verify that the SMI Status of the Communications Hub Function is not 'pending', 'installed not commissioned' or 'decommissioned', prior to raising an Incident.

5.4 Where any Communications Hub Availability and Diagnostics Check indicates that the SM WAN is unavailable for the Communications Hub, the Supplier Party shall check that there is no planned maintenance or existing DCC notified problem relating to SM WAN connectivity affecting the Installation Location by using the SM WAN network coverage functionality of the Self-Service Interface, prior to raising an Incident.

5.5 A Supplier Party shall include any relevant information from the Communications Hub Availability and Diagnostics Check in any Incident raised relating to that Communications Hub.

6. SPECIAL INSTALLATIONS & MODIFICATIONS

6.1 Where DCC identifies that resolution of an Incident relating to the ability to connect to the SM WAN requires work to be undertaken at a premises, the DCC shall notify the Supplier Party that raised the Incident accordingly. Such notification shall include details of the potential work required. The Supplier Party that raised the Incident may request that the DCC undertakes such work at the premises and the DCC shall be required to undertake such work, subject to the provisions of Section F7.5 – F7.7 of the Code.

6.2 Where a Supplier Party requires the DCC to undertake work at the premises, the Supplier Party shall update the Incident accordingly. The Supplier Party shall update the Incident with the following information when it is available:

(a) confirmation that consent for the work to be carried out has been obtained in accordance with Section F7.5 and F7.6 of the Code;

(b) the date and time at which the DCC should attend the relevant premises to carry out the work where;

(i) the Supplier Party shall ensure that the date shall be a Working Day, and the time shall be between 09:00 and 17:00;

(ii) the Supplier Party shall ensure that the date is no less than five (5) Working Days after the date of this update; and

(c) contact details that the DCC should use to confirm attendance prior to the agreed date and time or in the event that further liaison with the Supplier Party is required

(d) details of the reasoning for the need for DCC to attend.

6.3 Following the updates made pursuant to clause 6.2, the DCC shall subsequently update the Incident to provide contact details for its field force engineers at least one full Working Day prior to the date and time set for attendance at the relevant premises.

6.4 The DCC shall take all reasonable steps to attend the relevant premises at the specified date and time to undertake the work in accordance with Section F7.7 of the Code and shall notify the Supplier Party immediately where a delay to arrival is likely.

6.5 Where the DCC fails to meet the appointment, the DCC shall provide a list of reasonable options for revised dates and times from which the Supplier Party may select. Where the Supplier Party selects one of the potential dates and times offered by the DCC the provisions of clause 6.4 shall apply to that new date and time.

6.6 Where, in the Central Region and South Region, the DCC attends the relevant premises and identifies that T3 Aerial Type is required to resolve an Incident, the DCC shall:

(a) provide a T3 Aerial Type and any other equipment required to achieve connectivity between the Communications Hub and the SM WAN; and

(b) undertake such authorised work as is required to install such aerial and any additional required equipment.

6.7 Where, in the Central Region and South Region, the DCC attends the relevant premises and identifies that a Special Installation Mesh Communications Hub is required to resolve an Incident, the Supplier Party shall install a Special Installation Mesh Communications Hub provided by the DCC (as further set out in the CH Handover Support Materials) by following the fitting procedure set out in Annex A.1 of this document.

6.8 Following completion by the Supplier Party of the fitting procedure set out in Annex A.1 of this document for a Special Installation Mesh Communications Hub, the DCC shall:

(a) provide any aerial as deemed necessary (T1 Aerial Type, T2 Aerial Type, T3 Aerial Type, M1 Aerial Type or M2 Aerial Type) and any other equipment required to connect the Special Installation Mesh Communications Hub to the SM WAN; and

(b) undertake such work as is required to install such aerials or other equipment.

6.9 Where successful connection to the SM WAN is indicated, following installation of either:

(a) a Special Installation Mesh Communications Hub, with associated aerials and any additional required equipment:

or

(b) a T3 Aerial Type;

the Supplier Party shall complete the procedure set out in clause 4.7.

6.10 Where successful connection to the SM WAN is not achieved, following installation of a Special Installation Mesh Communications Hub, associated aerials and any additional required equipment, the Supplier Party may either:

(a) follow the fault handling procedure in accordance with clauses 8.3 to 8.6;

(b) leave the Special Installation Mesh Communications Hub installed without establishing a connection to the SM WAN by following the CH No SM WAN Installation Procedure; or

(c) remove the Special Installation Mesh Communications Hub in accordance with the process set out in Annex A of this document, in which case:

(i) the DCC shall remove all aerials and other equipment installed in accordance with 6.8(b);

(ii) the Supplier Party shall return the Special Installation Mesh Communications Hub to the DCC in accordance with clause 10.1 and in accordance with Section F7.4A;

(iii) the Supplier Party shall update the existing Incident with details of the steps that have been undertaken within three (3) Working Days; and

(iv) a notification shall be deemed not to have occurred for the purposes of Section F7.18.

6.11 Where a successful connection to the SM WAN is not achieved, following installation of a T3 Aerial Type and any additional required equipment, and where the DCC has decided not to require the Supplier to install a Special Installation Mesh Communications Hub, the Supplier Party may either:

(a) follow the fault handling procedure in accordance with clauses 8.3 to 8.6;

(b) leave the Communications Hub installed and connected to the T3 Aerial Type without establishing a connection to the SM WAN by following the CH No SM WAN Installation Procedure; or

(c) in accordance with any instruction from DCC, restore the Communications Hub aerial to its previous state, in which case:

(i) the DCC shall remove the T3 Type Aerial and other equipment installed in accordance with 6.8(b);

(ii) the Supplier Party shall update the existing Incident with details of the steps that have been undertaken within three (3) Working Days; and

(iii) a notification shall be deemed not to have occurred for the purposes of Section F7.18.

6.12 No Party other than the DCC may install, repair or remove T3 Type Aerials and/or M1 / M2 Type Aerials and other equipment installed in accordance with clause 6.8(b), without first seeking permission from DCC (save that such a Party may take action in accordance with Good Industry Practice to protect the health and safety of persons or to prevent imminent damage to property).

7. DCC REQUEST TO ATTEND A PREMISES

7.1 Where, in accordance with Section F7.13, DCC wishes to request permission to attend a premises at which a Communications Hub is installed, the DCC shall notify the Supplier Party from whom access is being requested. Such notification shall include:

(a) details of any premises which the DCC wishes to attend, and the nature of the activity or inspection that the DCC intends to conduct; and

(b) DCC email and telephone contact details for the Party to use in relation to the process of arranging attendance at the premises.

7.2 Where the Supplier Party agrees to a request from DCC in accordance Section F7.14, or is required to take all reasonable steps to obtain Energy Consumer consent in accordance with Section F7.15, the Party shall notify the DCC, using the contact details provided pursuant to clause 7.1(b), of the following:

(a) confirmation that consent for the work to be carried out has been obtained or notification that consent has not been obtained;

(b) where consent has been obtained, the date and time at which the DCC should attend the relevant premises where;

(i) the Supplier Party shall ensure that the date is a Working Day, and the time shall be between 09:00 and 17:00;

(ii) the Supplier Party shall ensure that the date is no less than thirty (30) Days after the DCC notification was issued in accordance with clause 7.1 or the Panel determination was made pursuant to Section F7.15; and

(c) contact details that the DCC should use to confirm attendance prior to the agreed date and time or in the event that further liaison with the Supplier Party is required.

7.3 Following notification to the DCC pursuant to clause 7.2, the DCC shall, using the contact details provided, inform the Supplier Party of contact details for their personnel at least one full Working Day prior to the date and time set for attendance at the relevant premises.

7.4 The DCC shall attend the relevant premises at the specified date and time and shall immediately notify the Supplier Party, using the contact details provided, where a delay to arrival is likely.

8. ON-SITE FAULT RESOLUTION AND COMMUNICATIONS HUB REPLACEMENT

Site Visit - Environment Check Procedure

8.1 Where a Supplier Party is at a premises and prior to undertaking any Communications Hub Fault Handling Procedures, or replacing a previously installed Communications Hub, a Supplier Party shall take all reasonable steps to verify that:

(a) the ICHIS compliant host is providing power to the Communications Hub; and

(b) that the prerequisites for installation of a Communications Hub set out in clauses 3.5 to 3.6 of this document are met.

8.2 Where the Supplier Party reasonably determines that the conditions in clause 8.1 are met the Supplier Party shall:

(a) where physical damage that is more than cosmetic is identified, remove the Communications Hub in accordance with clauses 9.1 to 9.9 of this document; and

(b) undertake the relevant Communications Hub Fault Handling Procedures.

Special Installation Mesh Communications Hub Fault Handling Procedures

8.3 Where following a remote fault diagnosis a Supplier Party reasonably assumes that a fault is attributable to a Special Installation Mesh Communications Hub or T3 Aerial Type or M1 / M2 Aerial Type, the Supplier Party shall raise or update an Incident in accordance with clause 6.2 to request that the DCC attends the Installation Location to resolve the Incident other than where DCC has indicated that that a site visit is not required to resolve the matter.

8.4 Where a Supplier Party is at a premises and a Special Installation Mesh Communications Hub, based on the CH Status Information, indicates an error state, and the Supplier Party reasonably determines that the either or both of the T3 Aerial Type or M1 / M2 Aerial Types (if installed) is at fault:

(a) where the DCC is in attendance, the DCC shall remove and replace either or both of the aerials immediately; or

(b) where the DCC is in not in attendance, the Supplier Party shall raise an Incident to request that the DCC undertakes such work at the premises and update the Incident with further information when it is available in accordance with clause 6.2.

8.5 Where a Supplier Party is at a premises and a Special Installation Mesh Communications Hub, based on the CH Status Information, indicates an error state, and the Supplier Party reasonably determines that the Special Installation Mesh Communications Hub is at fault, the Supplier Party shall:

(a) where the Supplier Party reasonably determines that the Special Installation Mesh Communications Hub can be removed and re-installed without disturbing either the installed T3 Aerial Type and/or M1 / M2 Aerial Types, take the following steps to remove and re-install the Communications Hub:

(i) disconnect the installed T3 Aerial Type and/or M1 / M2 Aerial Type;

(ii) remove the Communications Hub in accordance with clause 9 of this document;

(iii) following a period of no less than three (3) minutes, during which there is no physical connection to the host, re-install the same Communications Hub using the fitting and activation procedures as set out in A.1 and B.2 of this document, including the re-connection of the existing aerials;

(b) where having undertaken the activities set out in 8.5(a), the Special Installation Mesh Communications Hub, based on the CH Status Information, continues to indicate an error state; raise or update an Incident in accordance with clause 6.2 to request that the DCC attends the Installation Location to resolve the Incident

(c) where having undertaken the activities set out in 8.5(a), the Special Installation Mesh Communications Hub, based on the CH Status Information indicates a normal operating state: update any existing Incident with details of the steps that have been undertaken to resolve the Incident within three (3) Working Days.

8.6 Where the activities in clause 8.5(a) have been followed and the DCC is in attendance at the Installation Location, the Party shall then return the Special Installation Mesh Communications Hub in accordance with Section 10 of this document; and

(a) where the Party wishes to hand back the Special Installation Mesh Communications Hub the DCC shall accept the removed Communications Hub; and

(b) the DCC shall provide a replacement Special Installation Mesh Communications Hub immediately.

General Fault Handling Procedures

8.7 Where the Communications Hub (other than a Special Installation Mesh Communications Hub) based on the CH Status Information, indicates an error state, the Supplier Party shall ensure that:

(a) the Communications Hub is removed in accordance with clause 9 of this document; and

(b) following a period of no less than ten (10) seconds in the North Region and three (3) minutes in the Central Region and South Region, during which there is no physical connection to the host, the same Communications Hub is re-installed using the fitting and activation procedures as set out in Annex A and Annex B of this document.

8.8 Where, having undertaken the activities set out in clause 8.7, the Communications Hub (other than a Special Installation Mesh Communications Hub), based on the CH Status Information, continues to indicate an error state, and the Supplier Party wishes to resolve the fault, the Supplier Party shall ensure that:

(a) the Communications Hub is removed in accordance with clause 9; and

(b) a replacement Communications Hub is installed in accordance with the fitting and activation procedures set out in Annex A and Annex B of this document.

8.9 Where, having undertaken the activities set out in clause 8.7, the Communications Hub (other than a Special Installation Mesh Communications Hub), based on the CH Status Information indicates a normal operating state:

(a) update any existing Incident with details of the steps that have been undertaken to resolve the Incident within three (3) Working Days.

8.10 Where the Communications Hub is located within the Central Region or South Region and the Communications Hub, based on the CH Status Information, indicates an 'Attempting connect to the SM WAN' state for the maximum duration set out in the Communications Hub Supporting Information and the Communications Hub is a Cellular Communications Hub, the Supplier Party shall ensure that the following steps are undertaken when attempting to resolve the fault:

(a) the Communications Hub is removed in accordance with clause 9 of this document; and

(b) the fitting and activation procedures relevant to a Mesh Communications Hub are undertaken as set out in Annex A and Annex B of this document.

8.11 Where a Mesh Communications Hub (other than a Special Installation Mesh Communications Hub) is located within the Central Region or South Region and the Communications Hub, based on the CH Status Information, indicates an 'Attempting connect to the SM WAN' state for the maximum duration set out in the Communications Hub Supporting Information, the Supplier Party shall ensure that an aerial is fitted in accordance with the procedures set out in A.2 of this document.

SM WAN Connectivity

8.12 Where a Supplier Party determines that, having undertaken the relevant Communications Hub Fault Handling Procedure, no fault exists with a Communications Hub, but no SM WAN connection is achieved, that Supplier Party shall raise or update an Incident in accordance with the Incident Management Policy to inform DCC of a local SM WAN connectivity issue, subject to clause 8.13.

8.13 Prior to informing DCC of a local SM WAN connectivity issue a Supplier Party shall:

(a) ensure that the power supply to the Communications Hub is maintained following the completion of the fault handling procedure;

(b) verify that the Communications Hub Status Information does not indicate any fault other than failure to connect to the SM WAN; and

(c) ensure that the Communications Hub is fitted with a security seal.

9. COMMUNICATIONS HUB REMOVAL AND NOTIFICATION OF RETURNS

Communications Hub removal

9.1 A Supplier Party may remove a Communications Hub from an ICHIS compliant host that is powered.

9.2 Where a Supplier Party removes a Communications Hub and any associated Communications Hub Auxiliary Equipment, the Supplier Party shall do so in accordance with the procedures set out in Annex A of this document.

Notification of returns

9.3 Following the removal of a Communications Hub, as a result of a suspected or actual fault in the Communications Hub the Supplier Party shall notify the DCC of its removal by submitting a Service Request in accordance with clauses 9.4 or 9.5 as applicable within five (5) Working Days of the date of removal.

9.4 Where the Communications Hub has been removed due to physical damage, the Supplier Party shall submit a Service Request 8.14.3 (Communications Hub Status Update – Fault Return) indicating the appropriate fault return type and reason as specified in the DCC User Interface Specification (DUIS).

9.5 Where a Communications Hub is removed in accordance with clause 8.8, the Supplier Party shall submit a Service Request 8.14.3 (Communications Hub Status Update – Fault Return) indicating the appropriate fault return type as specified in the DUIS.

9.6 Where a Communications Hub is removed and clauses 9.4 and 9.5 do not apply, the Supplier Party shall submit a Service Request 8.14.4 (Communications Hub Status Update – No Fault Return) indicating the appropriate return type as specified in Section F9, within five (5) Working Days of the date of removal.

9.7 Where either:

(a) a Communications Hub is to be returned prior to installation pursuant to clause 3.4; or

(b) the DCC has requested the return of a Communications Hub in accordance with Section F8.1(b) of the Code or the Supplier Party is required to return pursuant to Section F8.6 of the Code;

the Party shall submit a Service Request 8.14.3 (Communications Hub Status Update – Fault Return).

9.8 Where a Communications Hub is to be returned prior to installation pursuant to Section F8.7(a) of the Code, the responsible Party shall submit a Service Request 8.14.4 (Communications Hub Status Update – No Fault Return).

9.9 In the event that a Party is not able to submit a Service Request in accordance with clauses 9.4, 9.5, 9.6, 9.7 or 9.8 that Party shall contact the Service Desk.

10. COMMUNICATIONS HUB RETURNS

10.1 Where a Supplier Party has handed back a Special Installation Mesh Communications Hub to the DCC whilst in attendance at the relevant premises and where the Special Installation Mesh Communications Hub had been installed at a previous installation visit, the Party shall submit Service Request 8.14.3 (Communications Hub Status Update – Fault Return) or Service Request 8.14.4 (Communications Hub Status Update – No Fault Return) in respect of the Communications Hub returned in accordance with DUIS within three (3) Working Days.

10.2 In all circumstances other than those specified in clause 10.1, including where a Party wishes to return a Special Installation Mesh Communications Hub or T3 Aerial Type and/or M1 / M2 Aerial Types when the DCC is not in attendance at the relevant premises in accordance with Section 6 of this document, the Party shall follow the procedure in clauses 10.3 - 10.20 of this document to return the Special Installation Mesh Communications Hub, and return the T3 Aerial Type and/or M1 / M2 Aerial Types within this process.

10.3 Following the acceptance of Communications Hubs, where a Party wishes to return Communications Hubs to the DCC, that Party shall do so in accordance with the procedures set out in clauses 10.1 to 10.20 of this document.

10.4 The DCC shall make available to all OMS account profiles, the following information for any DCC Returns Location:

(a) the full delivery address;

(b) operating hours; and

(c) the name, email address, and telephone number for a nominated contact in relation to Communications Hub returns.

Return Materials Authorisation

10.5 To return a Communications Hub a Party shall request a Returns Material Authorisation (RMA) once that Party has notified the DCC by either having:

(a) submitted Service Request 8.14.3 or Service Request 8.14.4 in respect of the Communications Hub to be returned; or

(b) contacted the Service Desk.

10.6 The requesting Party shall ensure that the request for an RMA is:

(a) made via the CH Ordering System; and

(b) includes:

(i) the CHF Identifier for each Communications Hub to be returned under that RMA, as previously notified to the DCC in accordance with clause 10.5

(ii) the contact name, email address, and telephone number to be used by the DCC to contact the Party in relation to that RMA;

(iii) the preferred DCC Returns Location; and

(iv) a preferred Return Date, which shall be on a Working Day at least five (5) Working Days following the date that the request for the RMA is submitted.

10.7 Following acceptance of an RMA request, the DCC shall:

(a) confirm authorisation to the submitting Party using the contact details provided;

(b) provide the Party with the following information via the Order Management System using either the 'CH Ordering' or 'CH Delivery and Returns' OMS profiles or via notification to the contact details provided:

(i) a unique booking reference;

(ii) confirmed timeslot for delivery;

(iii) RMA reference; and

(iv) any changes to the DCC contact details for the purposes of the return; and

(c) request any additional information as may be reasonably required to facilitate the logistics of the return in accordance with good industry practice.

Returns Equipment and Packaging

10.8 A Party shall ensure that all Communications Hubs returned to the DCC are in packaging of equivalent standard to that in which a Communications Hub of that Device Model was originally packaged, not exceeding the maximum number of Communications Hubs per carton and cartons per pallet set out in the CH Handover Support Materials.

10.9 A Party may return aerials or other equipment to DCC within a Communications Hub return delivery and must ensure that any aerials or other equipment returned to the DCC are in packaging of equivalent standard to that in which the aerials or other equipment was originally packaged.

10.10 Where a Communications Hub has been subject to environmental or biological contamination, the Party shall:

(a) where it is safe to do so, place the Communications Hub in appropriately sealed packaging such that DCC can clearly identify the nature of the contamination without removing or unsealing such packaging; or

(b) where safe return of a contaminated Communications Hub is not possible, safely and securely dispose of the Communications Hub.

Delivery of Returns

10.11 Where the Party does not return a Communications Hub within 90 days pursuant to Section F8.6 of the Code, the Communications Hub shall be deemed to be lost or stolen and the DCC shall prevent that Communications Hub from connecting to the SM WAN.

10.12 The Party shall ensure that the Communications Hub delivery is accompanied with a Return Delivery Note that contains, as a minimum, the following information:

(a) booking reference for the return delivery as supplied by DCC pursuant to clause 10.7;

(b) return date and return delivery time;

(c) Party Signifier;

(d) DCC Returns Location;

(e) list of all CHF Identifiers being returned; and

(f) (where one or more pallets are to be returned), the pallet identifiers for each pallet being returned.

10.13 The DCC shall provide the Party with a printable RMA label for each return delivery via the OMS (using the CH Ordering or CH Delivery and Returns profile) immediately following authorisation. The Party shall securely attach the corresponding RMA label on each pallet and each carton (where a carton is not part of a pallet) and each Communications Hub (where a Communications Hub is not part of a pallet or carton) for each return delivery.

10.14 The Party shall notify the DCC if there are any known issues that mean the delivery will be late, stating the reason for the delay and the expected time of arrival. The Party shall take all reasonable steps to make such notification a minimum of 5 Working Hours prior to the return delivery booking time. The DCC shall take all reasonable steps to accommodate a revised return delivery booking time and shall confirm to the Party that the DCC is either:

(a) able to accept the late return delivery; or

(b) unable to accept the return delivery.

10.15 Where the DCC is unable to accept the return delivery the DCC shall notify the returning Party as soon as reasonably practicable and shall notify the Party of the full range of available delivery dates and times within the following 90 days and the Party shall notify the DCC of an acceptable revised date and clauses 10.13 and 10.14 shall apply in relation to the revised date.

Delivery Acceptance

10.16 Prior to signing the Return Delivery Note, the DCC may carry out the following;

(a) assessment of pallets delivered against those recorded under the RMA request;

(b) checks between CHF Identifiers received against those listed under the RMA request; and

(c) checks that the number of Communications Hubs returned match the number of CHF Identifiers listed in the RMA request.

10.17 The DCC may reject any returned Communications Hubs where unloading them would present a health and safety risk. Where the DCC rejects the return delivery, the Party shall be required to request a new RMA and rearrange the return delivery following the relevant procedures set out in clauses 10.5 to 10.15 of this document.

10.18 Following the checks performed pursuant to clause 10.16, the DCC shall record any discrepancies between the return delivery and the Return Delivery Note.

10.19 Where requested to do so the DCC shall sign and retain a copy of the Return Delivery Note.

10.20 Where the Party fails to provide the DCC with a fault reason for each CHF Identifier in accordance with the requirements set out in this document, the Communications Hub shall be deemed to be a return pursuant to Section F9.5 (e) of the Code and the Communications Hub Fault shall be a CH User Responsibility in accordance with Section F9.6 (a) of the Code.

11. CH FAULT DIAGNOSIS BY DCC

Receipt of Communications Hubs

11.1 The DCC shall create an individual record for each returned Communications Hub on receipt of Service Request 8.14.3, 8.14.4 or any return notified through the Service Desk. For each returned Communications Hub this record shall contain all details received by DCC from the Party within the Service Request or provided via the Service Desk and other supporting information as set out in Annex D, and shall be made available by the DCC to the Party that returned the Communications Hub within seven (7) days after the return of the Communications Hubs via the CH Ordering System.

Notification

11.2 Where the DCC intends to undertake any CH Fault Diagnosis, the DCC shall update the relevant record, as described in Annex D of this document, indicating that further analysis is required, in accordance with Section F9.9 of the Code. The DCC shall make this information available and notify the Party that returned the Communications Hub within ten (10) days after the return of the Communications Hubs or notification of its loss or destruction pursuant to Section F9.9, of this revision.

11.3 In the event that a Party is not able to access the record created in accordance with clause 11.1, that Party may contact the Service Desk in order to access the record, which the DCC shall enable.

Fault Diagnosis Approach

11.4 The DCC shall undertake CH Fault Diagnosis using visual and electronic analysis of returned Communications Hubs, as set out in clauses 11.5 and 11.6.

Visual analysis

11.5 The DCC may undertake the following visual inspections of a returned Communications Hub and shall subsequently update the information in the record created pursuant to 11.1 to include the results from this analysis:

(a) check for any physical damage to any part of the Communication Hub including, but not limited to, the outer casing, external interfaces and connectors;

(b) check to identify any loose internal components and for evidence that such components were previously connected correctly;

(c) check for any evidence of tampering; and

(d) check for any evidence of exposure to adverse environmental conditions including, but not limited to, water, condensation, smoke, chemicals, pests, etc.

Electronic analysis

11.6 Where the Communications Hub is not deemed to be physically damaged in accordance with clause 11.5, the DCC may undertake the electronic diagnostic tests described in Annex C of this document and shall subsequently update the information in the record created pursuant to 11.1 to include the results from this analysis.

Fault Analysis Report

11.7 Pursuant to Section F9.11, where the DCC disputes the reason given by a Party for the return of a Communications Hub, the DCC shall provide the Party which returned the Communications Hub with a report. The DCC shall provide this report by updating the relevant Fault Analysis Report record maintained for each returned Communications Hub, as set out in Annex D of this document, with the results of the Fault Analysis and make this available via the CH Ordering System and notify the Party that returned the Communications Hub.

Acceptance

11.8 Where the DCC provides a Fault Analysis Report and the Party does not object in accordance with Section F9.13 of the Code, no further action is required by the Party and the DCC shall update the 'Returns Record Status' field to "Closed".

Objections

11.9 Where the Party wishes to notify the DCC of their objection pursuant to Section F9.14 of the Code it shall do so via the Service Desk.

Annex A. CH Fitting and removal procedures

A.1. Fitting procedure

A.1.1 A Party shall ensure that all reasonable precautions are taken to avoid electrostatic discharge whilst handling the Communications Hub.

A.1.2 A Supplier Party shall ensure that all reasonable precautions are taken to avoid electrostatic discharge when installing any Communications Hub and Communications Hub Auxiliary Equipment.

A.1.3 The Communications Hub shall be mounted vertically above the ICHIS compliant host, ensuring that the Communications Hub Variant labelling text on the front face is horizontal.

A.1.4 A Party may mount a Communications Hub on an ICHIS compliant host that is powered.

A.1.5 A Supplier Party shall fit a Communications Hub in accordance with the steps set out below:

(a) **Step 1 -** Align Communications Hub guide rails with the U-channel of the ICHIS compliant host;

(b) **Step 2 -** Slide the Communications Hub on to the ICHIS compliant host, ensuring that the Communications Hub guide rails remain within the U-Channel of the ICHIS compliant host;

(c) **Step 3 -** Press the front faceplate in order to connect the Communications Hub to the interface of the ICHIS compliant host, applying hand pressure only; and

(d) **Step 4 -** Screw in the M4 retaining screw located on the front faceplate of the Communications Hub to fasten it to the ICHIS compliant host.

A.2. Installation of Communications Hub aerials - Central Region and South Region

A.2.1 For the South Region or Central Region, where a Communications Hub (as indicated by the Coverage Database) requires an aerial (T1 Aerial Type or T2 Aerial Type), or where an aerial is required as a result of a failure as described in B.2.4 of this document, the Supplier Party shall ensure that a Mesh Communications Hub is installed and that when installing an aerial:

(a) all reasonable steps are taken to ensure any aerial (T1 Aerial Type or T2 Aerial Type) is positioned vertically and avoiding any Significant Metallic Obstruction;

(b) all reasonable steps to minimise risk of damage to the aerial lead during installation are undertaken and that the environmental conditions for the Communications Hub as defined in Annex C of the CH Handover Support Materials are not exceeded;

(c) stub aerials (i.e. with no cable attached) are not used to connect the aerial directly onto the Communications Hub, the cable must always be used as supplied.

A.2.2 For the South Region or Central Region, a Supplier Party shall:

(a) first attempt to install a standard Communications Hub T1 Aerial Type in accordance with the installation steps set out in A.2.3; and

(b) where, in step 6 (A.2.3(f)), the minimum signal strength required as indicated by the Visual Information set out in the CH Supporting Information is not obtained, the Party shall remove the T1 Aerial Type and install a T2 Aerial Type in accordance with the installation steps set out in A.2.3.

A.2.3 A Supplier Party shall install a Communications Hub aerial in accordance with the steps below:

(a) **Step 1 -** unpack the aerial and inspect for damage;

(b) **Step 2 -** attach the aerial to the cable SMA connector, if the cable is not supplied already integrated with the aerial;

(c) **Step 3 -** ensure the Communications Hub is powered up and fully initialised when connecting the aerial and cable to the SMA connector on the Communications Hub;

(d) **Step 4 -** fasten all SMA connectors to finger-tightness;

(e) **Step 5 -** secure the Communications Hub hinged plastic cover over the connector, ensuring that the aerial cable routes through the provided aperture on the base of the cover and remains free to allow aerial positioning once fitted;

(f) **Step 6 -** for connection of a T1 Aerial Type, T2 Aerial Type or T3 Aerial Type only, use the Visual Information set out in the CH Supporting Information to identify the strength of the signal at varying positions of the aerial and cable to first maximise the signal strength and second minimise the distance to the Communications Hub;

(g) **Step 7 -** if the aerial position does not require the full length of the supplied aerial cable, the spare aerial cable shall be loosely coiled and fastened using a fabric hook- and-loop cable tie ensuring not to crush or kink the aerial cable;

(h) **Step 8 -** for connection of a T1 Aerial Type, T2 Aerial Type or T3 Aerial Type only, once the optimum location for the aerial has been confirmed the aerial shall be positioned vertically with the cable connector at the base then either:

(i) fasten the aerial in place using the appropriate fasteners provided in the assembly kit: or

(ii) depending on the type of aerial used, connect to a wall using self-adhesive.

(i) **Step 9 -** following installation of the aerial as set out in steps 1-8 above, the installer should wait for a minimum of two (2) minutes, and then undertake the activation processes set out in Annex B of this document.

A.2.4 For the South Region or Central Region, where a Special Installation Mesh Communications Hub is to be installed and requires an aerial (T1 Aerial Type or T2 Aerial Type and M1 Aerial Type), or where an aerial is required as a result of a failure as described in B.2.4 of this document, the Supplier Party shall ensure that a Special Installation Mesh Communications Hub is installed and that when installing an aerial:

(a) all reasonable steps are taken to ensure any aerial (T1 Aerial Type, T2 Aerial Type or M1 Aerial Type) is positioned vertically and avoiding any Significant Metallic Obstruction;

(b) all reasonable steps to minimise risk of damage to the aerial lead during installation are undertaken and that the environmental conditions for the Communications Hub as defined in Annex C of the CH Handover Support Materials are not exceeded;

(c) stub aerials (i.e. with no cable attached) are not used to connect the aerial directly onto the Communications Hub, the cable must always be used as supplied;

A.2.5 For the South Region or Central Region, where a Special Installation Mesh Communications Hub is to be installed and requires an external aerial (T3 Aerial Type or M1 / M2 Aerial Types), or where an aerial is required as a result of a failure as described in B.2.4 of this document, the Supplier Party shall ensure that a Special Installation Mesh Communications Hub is installed and that when installing an external aerial, the manufacturer's instructions for selecting the installation position and mounting the aerials are followed, particularly with reference to the following:

(a) The aerial must be mounted in a vertical plane with the cable exiting from the bottom,

(b) The aerial should be located such that the distance to any nearby device or metal structure should exceed the stated minimum distance. The aerial must not be installed on or close to a metal panel,

(c) The aerial should be mounted in such a way that no person is likely to be within the RF exclusion zone while the aerial is in use,

(d) If both the T3 Aerial Type and M2 Aerial Types are specified for installation on the external wall of a property, the T3 Aerial Type should be mounted vertically above the M1 / M2 Aerial Types such that the minimum vertical separation between them is met or exceeded,

(e) Only those brackets and fittings supplied by the manufacturers should be used for installing the T3 Aerial Type or M1 / M2 Aerial Types.

A.3. Communications Hub removal procedure

A.3.1 Where a Supplier Party removes a Communications Hub, the Supplier Party shall:

(a) **Step 1 -** Remove or break the security seal;

(b) **Step 2 -** Remove the M4 retaining screw located on the front faceplate of the Communications Hub to enable its removal from the ICHIS compliant host; and

(c) **Step 3 -** Slide the Communications Hub from the ICHIS compliant host, ensuring that the Communications Hub guide rails remain within the U-Channel of the Electricity Smart Meter, Cradle or Hot Shoe.

Annex B. Activation Procedure

B.1. Communications Hub Activation Procedure - North Region

B.1.1. For the North Region, following the fitting of a Communications Hub, the Supplier Party shall verify the successful activation of the Communications Hub by monitoring that the CH Status Information indicates the following Communications Hub states as set out in the CH Supporting Information, in the sequence:

(a) 'SM WAN initialising';

(b) 'Attempting to connect to the SM WAN'; and

(c) 'SM WAN connected'.

B.1.2. For the North Region, where the Communications Hub activation fails to complete, the Supplier Party shall ensure that:

(a) where the CH Status Information indicates that the Communications Hub is in an error state, the Communications Hub Fault Handling Procedures are followed; or

(b) where the Communications Hub fails to transition from the 'Attempting connect to the SM WAN' state to the 'SM WAN connected' state within the maximum time set out in the CH Supporting Information, but no fault is indicated, the Supplier Party may wish to undertake the CH No SM WAN Installation Procedure.

B.2. Communications Hub Activation Procedure - Central Region and South Region

B.2.1. Following the fitting of a Cellular Communications Hub, the Supplier Party shall ensure that a check is performed to confirm that the following Communications Hub states are achieved, based on the CH Status Information, as set out in the CH Supporting Information:

(a) initialisation complete ('Device initialising' transition steps complete successfully);

(b) SW LED 'Normal operating state';

(c) WAN LED 'Attempting connect to SM WAN'; and

(d) WAN LED 'SM WAN connected'.

B.2.2. Where the Communications Hub activation fails to complete, the Supplier Party shall ensure that:

(a) where the CH Status Information indicates that the Communications Hub is in an error state (SW LED 'Device in error state' or WAN LED 'SM WAN error'), the fault resolution procedures set out in clauses 8.1 to 8.13 of this document are followed; or

(b) where the WAN LED indicator fails to transition from the 'Attempting connect to SM WAN' state to the 'SM WAN connected' state within the maximum time set out in the CH Supporting Information, the Cellular Communications Hub is removed and a Mesh Communications Hub is fitted in accordance with the fitting and activation procedures set out in Annex A and Annex B of this document.

B.2.3. Where installing a Mesh Communications Hub or Special Installation Mesh Communications Hub, the Supplier Party shall ensure that the Visual Information set out in the CH Supporting Information is monitored to confirm the following Communications Hub states are achieved:

(a) initialisation complete ('Device initialising' transitions complete successfully);

(b) SW LED showing 'Normal operating state';

(c) and either:

(i) SM WAN (cellular) - WAN LED showing 'Attempting connect to SM WAN';

(ii) SM WAN (cellular) - WAN LED showing 'SM WAN connected';

or

(iii) Mesh - MESH LED showing 'Attempting to connect to Mesh'; and

(iv) Mesh - MESH LED showing 'Mesh connected'.

B.2.4. Where the Mesh Communications Hub activation fails to complete, the Supplier Party shall ensure that:

(a) where the CH Status Information indicates that the Mesh Communications Hub is in an error state, the fault resolution procedures set out in clauses 6.1 to 6.5 of this document are followed; and either:

(b) where no Communications Hub T2 Aerial Type has previously been fitted and the WAN LED indicator fails to transition from the 'Attempting connect to SM WAN' state to the 'SM WAN connected' state or from the 'Attempting to connect to Mesh' state to the 'Mesh connected' state within the maximum time set out in the CH Supporting Information, a Communications Hub T2 Aerial Type is fitted in accordance with the fitting and activation procedures set out in Annex A and Annex B of this document.

or

(c) where a Communications Hub T2 Aerial Type has previously been fitted and the Mesh Communications Hub fails to transition from the 'Attempting to connect to SM WAN' state to the 'SM WAN connected' state or from the 'Attempting to connect to Mesh' state to the 'Mesh connected' state within the maximum time set out in the CH Supporting Information, but no fault is indicated, the Supplier Party may wish to undertake the CH No SM WAN Installation Procedure.

Annex C. Electronic Fault Diagnosis

C.1.1. The DCC may carry out the following checks as part of the Communications Hub Fault Handling Procedure:

a) check of hardware and firmware;

b) check of device configuration;

c) checks of power consumption;

d) detection of malfunction of internal components via self-tests;

e) connectivity test for HAN components;

f) connectivity test for SM WAN components;

g) functional check of visual status indicators (LEDs);

h) verification that power outage power storage is within expected tolerance;

i) tamper detection check;

j) clock test (set real-time clock or read real-time clock); and

k) review of the security and event logs.

Annex D. Fault Analysis Report – fault record data items

D.1.1. Table 1 identifies the data fields that will be provided in the Communications Hub Fault Analysis Report. Data items shall be updated in line with the progress of the fault analysis and some items may therefore be blank.

Table 1; Fault Analysis Report – fault record data field descriptions

Field name	Description
Returns record id	Unique reference for the returns Record.
Incident reference	This field displays the Incident request identifier if provided by a Party
User ref id	Unique reference for the update provided by a Party.
User id	SEC Party Signifier of the Party that submitted the Communications Hub status update
CHF return type	Category of Return, as provided by a Party and specified in DUIS
User fault diagnosis (CHF fault reason)	Initial fault diagnosis code, as provided by a Party and specified in DUIS.
CSP fault diagnosis	DCC fault diagnosis following the fault analysis process.
DCC fault diagnosis	DCC fault diagnosis following conclusion of any objection process.

User fault responsibility	Derived from user fault diagnosis
CSP fault responsibility	DCC fault responsibility derived from DCC fault diagnosis
Final agreed fault responsibility	Derived from DCC fault diagnosis
CSP id	The DCC Service Provider identified by the Region.
Device id	The unique CHF ID
Return record create date	The Date and time the returns record was created.
User job date time	Time of removal of the Communications Hub provided by a Party.
Preliminary FAR received date	The date the DCC updated the record to issue the preliminary Fault Analysis Report.
CSP FAR received date	The date the DCC issued the final Fault Analysis Report.
Return closed date	The date and time the DCC issued the final Fault Analysis Report.
Received communications hub date	The date and time the DCC receives the Communications Hub from the Party.
Dispute start date	The date and time the dispute was notified to DCC and the record status was updated to 'In Dispute'.
Other device id	UID of the ESME or GSME
CHF connection method	To record whether hot-shoe or cradle CHF installation
	To record how the Communications Hub has been installed and connected to the rest of the Smart Metering System within the premises Valid set: Hot-shoe Cradle ESME
Cause of fault	A short description of the fault cause supplied by the DCC

Additional information	Further Analysis details from the Fault Cause supplied by the DCC
Full analysis	Y/N flag indicating whether a full analysis is required. Will drive the status of the returns record
User organisation	Details of organisation associated with User ID
Premises postcode	Derived from MPAN / MPRN associated with the Communications Hub
Product name	Derived from CHF ID
Model	Derived from CHF ID
Manufacturer	Derived from CHF ID
Communications hub delivery location	The location the Communications Hub was delivered to (provided by DCC)
Communications hub installation date	From the Smart Metering Inventory, where applicable.
Incident resolved date	Manually populated by Service Desk
CSP region	The Region in which the Communications Hub was installed.
Communications hub commissioned date	From the Smart Metering Inventory
Communications hub device type	Supplied on creation by DCC
Communications hub returning supplier	Supplied on creation by DCC
Communications Hub delivery date	From the Smart Metering Inventory.

Annex E. Equipment Supplied

E.1. North Region

E.1.1. The DCC shall supply the following equipment, which can be ordered via the OMS:

a) ‘Standard 420’ Communications Hub Variant with captive security screw; and

b) ‘Standard 420 DB’ Communications Hub Variant with captive security screw; and

c) ’Variant 450 DB’ Communications Hub Variant with captive security screw.

E.2. Central and South Regions

E.2.1 The DCC shall supply the following equipment, which can be ordered via the OMS:

a) ‘SKU1 Cellular’ Communications Hub Variant with captive security screw; and

b) ‘SKU2 Cellular + Mesh’ Communication Hub Variant with captive security screw; and

c) ‘Cellular DB’ Communications Hub Variant with captive security screw; and

d) ‘Cellular + Mesh DB’ Communications Hub Variant with captive security screw; and

e) Communications Hub Auxiliary Equipment, including aerials, aerial cable and fabric hook-and-loop ties, two aerial types shall be provided:

e)1 T1 Aerial Type; and

e)2 T2 Aerial Type.

E.2.2 The DCC shall supply the following equipment directly at joint visits:

a) ‘SKU3 SIMCH’ (Special Installation Mesh Communications Hub) Communications Hub Variant with captive security screw; and

b) ‘SIMCH DB’ Communications Hub Variant with captive security screw; and

c) Up to three aerial types and related cables and fixings shall be provided:

i) T3 Aerial Type

ii) M1 Aerial Type

iii) M2 Aerial Type

E.2.3 All Communications Hub Variants, their HAN/WAN Variant attributes and CSP Regions are listed in table 2.

Table 2; Summary of all Communications Hub Variants with their HAN/WAN Variant attributes and CSP Regions

CH Variant	HAN Variant	WAN Variant	CSP Region
Standard 420	Single Band (2.4GHz only)	420	CSP North
Standard 420 DB	Dual Band (868MHz and 2.4GHz)	420	CSP North
Variant 450 DB	Dual Band (868MHz and 2.4GHz)	450	CSP North

SKU1 Cellular	Single Band (2.4GHz only)	Cellular	CSP South & Central
SKU2 Cellular + Mesh	Single Band (2.4GHz only)	Cellular+Mesh	CSP South & Central
SKU3 SIMCH	Single Band (2.4GHz only)	Special Installation Mesh	CSP South & Central
Cellular DB	Dual Band (868MHz and 2.4GHz)	Cellular	CSP South & Central
Cellular + Mesh DB	Dual Band (868MHz and 2.4GHz)	Cellular+Mesh	CSP South & Central
SIMCH DB	Dual Band (868MHz and 2.4GHz)	Special Installation Mesh	CSP South & Central

868MHz means, for the purposes of the Code, sub-GHz

E.3. Communications Hub WAN Variant Values

E.3.1 For the purpose of providing WAN Technology values for use with the 12.1 RequestWANMatrix Service Request as detailed in APPENDIX AD ‘DCC User Interface Specification’, Communications Hub WAN Variant values are listed in table 3

Table 3; Summary of all Communications Hub WAN Variants for use with Service Request 12.1

WAN Variant (DCC 1.3)	WAN Variant (DCC 2.0)	CSP Region
Standard 420	420	CSP North
Variant 450	450	CSP North
Cellular	Cellular	CSP South & Central
Cellular+Mesh	Cellular+Mesh	CSP South & Central
No Coverage Intended	No Coverage Intended	N/A
" " Space	" " Space	CSP South & Central

To note: on Table 3, " " Space above, CSP South & Central will respond to a SMWAN Coverage request (CSPM-S1 or CSPM-S2) with an Availability Date for coverage but without confirming the WAN Variant that

will need to be used. Upon receipt of this WAN Variant, the Service User will read “ “ Space as WAN Variant unknown.

Version J 7.0

Appendix J

Enduring Testing Approach Document

1. Introduction

Scope

1.1 The Enduring Testing Approach Document (ETAD) describes the detailed procedural and technical requirements for the Testing Services, as defined in Section H14.1 of this Code, that the DCC will make available to Testing Participants on an enduring basis. Unless indicated otherwise this ETAD applies to Testing Services in respect of SMETS1 Devices and SMETS2+ Devices

2. Security Requirements

2.1 For the purposes of this document, "Testing Participant Systems" means:

(a) any Systems (excluding any Devices) that are operated by or on behalf of a Testing Participant and used in whole or in part for the testing equivalent of:

(i) constructing Service Requests;

(ii) sending Service Requests over the DCC User Interface;

(iii) receiving, sending, storing, using or otherwise carrying out any processing in respect of any Pre-Command or Signed Pre-Command;

(iv) receiving Service Responses or Alerts over the DCC User Interface;

(v) generating Data for communication to the OCA, DCA or ICA, or receiving Data from the OCA, DCA or ICA (including any Systems which store or use Secret Key Material for such purposes) but only communications in relation to Devices that have an SMI Status of "commissioned" or "installed not commissioned";

(vi) generating any Unique Transaction Reference Number;

(vii) providing (or procuring the provision of) Registration Data in respect of a particular MPAN or MPRN; and/or

(viii) the collection, storage or communication of the Registration Data referred to in sub-clause vii) above prior to, or for the purposes of, its provision to DCC over the Registration Data Interface; and

(b) any other Systems from which the Systems used in whole or in part for the purposes set out in clause (a) are not Separate.

2.2 Each Testing Participant shall ensure that its Testing Participant Systems are Separate from:

(a) its RDP Systems or User Systems, as appropriate; and

(b) any other Systems not used for the purposes of carrying out tests using the Testing Services.

2.3 Each Testing Participant shall take reasonable steps to ensure that:

(a) its Testing Participant Systems are capable of detecting any unauthorised software that has been installed or executed on them and any unauthorised attempt to install or execute software on them;

(b) if those Testing Participant Systems detect any such software or such attempt to install or execute software, that the installation or execution of that software is prevented; and

(c) where any such software has been installed or executed, to take appropriate remedial action.

2.4 Each Testing Participant shall ensure that it carries out assessments that are designed to identify any vulnerability of its Testing Participant Systems to Compromise:

(a) prior to accessing any Testing Services using such Testing Participant Systems and on at least an annual basis thereafter;

(b) in respect of each new or materially changed component or functionality of its Testing Participant Systems, prior to that component or functionality becoming operational; and

(c) on the occurrence of any security issue in relation to its Testing Participant Systems.

2.5 Where, following any assessment of its Testing Participant Systems in accordance with clause 2.4 or otherwise, any material vulnerability has been detected, the Testing Participant shall:

(a) take reasonable steps to ensure that the cause of the vulnerability is rectified, or the potential impact of the vulnerability is mitigated, as soon as is reasonably practicable; and

(b) promptly notify the DCC of the steps being taken to rectify its cause or mitigate its potential impact (as the case may be) on DCC Systems and the time within which they are intended to be completed, and comply with any reasonable request from the DCC to mitigate or prevent any potential adverse impact on the DCC Systems arising from such vulnerability.

3. IKI and SMKI Test Certificates

3.1 The DCC shall issue Test Certificates simulating the function of Organisation Certificates, OCA Certificates, Device Certificates, DCA Certificates, IKI Certificates and ICA Certificates in accordance with the relevant provisions of the “Test Documents”.

3.2 For the purposes of clause 3.1, the Test Documents means:

(a) the Test Certificate Policy, which shall be a document published on the DCC Website and approved by the SMKI PMA which corresponds (insofar as relevant in respect of the Testing Services) in purpose, content and effect to the Organisation Certificate Policy, the Device Certificate Policy and the IKI Certificate Policy; and

(b) subject to clauses 3.3 and 3.4:

(i) the SMKI RAPP;

(ii) the SMKI Interface Design Specification;

(iii) the SMKI Code of Connection;

(iv) the SMKI Repository Interface Design Specification; and

(v) the SMKI Repository Code of Connection.

3.3 For the purposes of clause 3.2(b) (i), each Testing Participant shall, when completing the forms in the appendices of the SMKI RAPP for test purposes, clearly mark each page with the text, “For Testing Purposes” and submit the completed forms to the SMKI Registration Authority, in writing, as directed on the DCC Website.

3.4 For the purposes of clause 3.2(b):

(a) any reference in such documents to any office, function, role, system, process or other thing shall be construed as being a reference to the corresponding equivalent of that office, function, role, system, process or thing which is established, undertaken, operated or given effect (as the case may be) for the purposes of the Testing Services;

(b) Testing Participants shall not be required to complete SMKI and Repository Entry Process Tests to become eligible to obtain IKI and SMKI Test Certificates;

(c) where agreed by the DCC and a Testing Participant, any of the requirements that a Testing Participant must satisfy in order to be entitled to become an Authorised Subscriber for a Test Certificate may be disregarded for the purposes of such entitlement;

(d) the DCC shall publish on the DCC Website, and from time to time update, limits on the number of Certificate Signing Requests that each Testing Participant may submit in any particular time period over any relevant interface for testing purposes;

(e) each Testing Participant shall take all reasonable steps to ensure it does not submit certificate signing requests for testing purposes in excess of any limit published (or updated) in accordance with clause (d) above;

(f) the DCC shall publish on the DCC Website, and from time to time update, limits on the total number of Certificate Signing Requests across all Testing Participants that can be processed each day. The DCC shall not be required to process any Certificate Signing Request in excess of such limits that is submitted by any Testing Participant.

4. DCCKI Test Certificates

4.1 The DCC shall issue DCCKI Test Certificates simulating the function of DCCKI Certificates in accordance with the relevant provisions of the “DCCKI Test Documents”. A separate DCCKI Test Certificate will be required for each test environment.

4.2 For the purposes of clause 4.1, the DCCKI Test Documents means, subject to clauses 4.3 and 4.4:

(a) the Test DCCKI Certificate Policy;

(b) the DCCKI RAPP;

(c) the DCCKI Interface Design Specification and DCCKI Repository Interface Design Specification; and

(d) the DCCKI Interface Code of Connection and DCCKI Repository Code of Connection.

4.3 For the purposes of clause 4.2 (a) and for issuing Test DCCKI Certificates, the Test DCCKI Certificate Policy shall be the most recent DCCKI Certificate Policy at that date, modified such that:

(a) the OID in clause 1.2 is replaced by 1.2.826.0.1.8641679.1.2.1.12

(b) the modifications identified in clause 4.5 below apply; and

(c) any changes that:

(i) have been approved by the DCCKI PMA function prior to taking effect; and

(ii) do not directly affect any rights or obligations of Parties (other than the DCC) or RDPs, apply.

4.4 For the purposes of clause 4.2:

(a) any reference in such documents to any office, function, role, system, process or other thing shall be construed as being a reference to the corresponding equivalent of that office, function, role, system, process or thing which is established, undertaken, operated or given effect (as the case may be) for the purposes of the Testing Services;

(b) Parties and RDPs shall be considered to be DCCKI Authorised Subscribers for testing purposes where they have appointed at least one DCCKI SRO and at least one DCCKI ARO;

(c) any reference to lodging of information in the DCCKI Repository, including DCCKI Certificates, EII DCCKICA CRL and DCCKI ARL, shall be modified such that the DCC may, where the DCCKI Repository is not available, provide such information via an alternative means to be notified to DCCKI Authorised Subscribers, and where approved in advance by the DCCKI PMA function;

(d) all obligations on the DCC in respect of timescales associated with the delivery of DCCKI Services or DCCKI Repository Services, shall be modified so that any such timescales shall be replaced with “as soon as reasonably practicable, having regard to the requirement to provide DCCKI Services and DCCKI Repository Services”;

(e) any reference to raising Incidents and Major Security Incidents shall not apply and the provisions of the Testing Issue Resolution Process shall apply; and

(f) the following provisions of the documents shall be disregarded and treated as forming no part of the DCCKI Test Documents:

(i) references to interactions with the Service Desk processes shall not apply, except to the extent that such processes are required to support the identity verification of individuals nominated to become DCCKI SROs or DCCKI AROs for testing purposes; and

(ii) clauses 3.2 (b); 3.15; 3.16; and 4.4 to 4.12; in the DCCKI RAPP shall not apply.

4.5 For the purposes of clause 4.2(b), each Testing Participant shall, when completing the forms in the annexes of the DCCKI RAPP for testing purposes, clearly mark each page with the text, “For Testing Purposes” and submit the completed forms to the DCCKI Registration Authority, in writing, as directed on the DCC Website.

5. Obligations on Testing Participants using Remote Test Labs

5.1 In accordance with Section H14.31, Testing Participants are eligible to connect to a simulation of the SMETS2+ SM WAN ("a test SMETS2+ SM WAN") for the purposes of conducting Device and User System Tests remotely at premises of their choice. The DCC shall offer a service of providing connections to the test SMETS2+ SM WAN, but shall not offer such service in respect of the SMETS1 SMWAN. However, where a Testing Participant is able to arrange for its own connection to a simulation of the SMETS1 SM WAN ("test SMETS1 SM WAN"), that Testing Participant shall be entitled to conduct Device and User System Tests remotely at premises of their choice.

SMETS 2+

5.2 As well as providing the necessary Test Communications Hubs, Smart Meters and any other Devices which they choose to test, the Testing Participant may need to establish a connection to the test SMETS2+ SM WAN (in the chosen Region(s)). DCC will provide separate testing environments to support fix on fail and development activities. Testing Participants will need to establish connections to the environments they choose to test in.

5.3 The DCC shall include a description of the equipment that will be provided to enable connection to and use of a test SMETS2+ SM WAN for the purposes set out above in the guide for Testing Participants which the DCC is obliged to publish under Section H14.3.

5.4 Where a Testing Participant is considering ordering a connection to the test SMETS2+ SM WAN, the Testing Participant shall first contact the DCC via the Service Desk to request a site survey and resulting quotation setting out the charges to apply. For each additional Remote Test Lab connection to a specific testing environment, a site survey may be required.

5.5 When seeking a connection to the SMETS2+ SM WAN, a Testing Participant shall comply with any reasonable requests of the DCC to provide supporting information, which may include but not be limited to:

(a) location of the site which needs to be connected;

(b) an estimate of the number of Test Communications Hubs, Electricity Meters and Gas Meters that the Testing Participant wishes to install in its test facility and each testing environment; and

(c) a digital floor plan including the area surrounding the test facility, including dimensions, floors above and below and outside windows.

5.6 On receiving a request for a site survey and a quotation of the charges to apply for connection to the test SMETS2+ SM WAN, the DCC shall undertake the steps detailed below as soon as is reasonably practicable:

(a) conduct a site survey to assess the equipment that needs to be provided by the DCC, and any specific requirements to be fulfilled by the DCC for the premises at which the equipment is to be installed. For this purpose, the Testing Participant shall provide the DCC personnel with access to its site to enable the DCC to conduct a site survey; and

(b) set out the charges to apply, which may comprise:

(i) a connection charge for standard connection equipment;

(ii) an additional charge for additional, non-standard connection equipment; and

(iii) a monthly operating charge.

5.7 Upon receipt of the details of the site survey and the charges which will apply, the Testing Participant shall, if it wishes to place an order, notify the DCC accordingly within 30 days of receipt. Any dispute relating to the charges specified by the DCC shall be resolved in accordance with Section M7.2(d).

5.8 Where the Testing Participant notifies the DCC that it wishes to place an order under clause 5.70, the DCC shall provide the connection as soon as is reasonably practicable, and in any event within 6 months of the order being placed.

5.9 The DCC shall provide reasonable notice to the Testing Participant of the planned date of installation of the connection equipment and the establishment of the connection to the test SMETS2+ SM WAN.

5.10 Where the Testing Participant requests a change to the planned date of installation advised by the DCC, that planned date of installation shall be amended, subject to the Testing Participant agreeing to pay for any additional charges notified by the DCC to cover the additional reasonable costs incurred by the DCC resulting from the change of date. In first providing the connection at the premises, the DCC shall procure that the test SMETS2+ SM WAN connection equipment is installed at the premises and that it is done so in accordance with Good Industry Practice and all applicable Laws and Directives.

5.11 A Testing Participant at whose premises test SMETS2+ SM WAN connection equipment has been installed shall implement and maintain reasonable controls to ensure the physical security of the equipment and ensure that no damage is deliberately or negligently caused to that equipment (save that such a Party may take emergency action in accordance with Good Industry Practice to protect the health and safety of persons or to prevent imminent damage to property).

5.12 The test SMETS2+ SM WAN connection equipment shall (as between the DCC and the Testing Participant) remain the property of the DCC, and shall form part of the DCC System. No Testing Participant shall hold itself out as the owner of such connection equipment, or purport to sell or otherwise dispose of such connection equipment. Such equipment is installed at the DCC's risk and no Testing Participant shall have liability for any loss or damage to the equipment unless and to the extent that such loss or damage arose as a result of that Testing Participant's breach of this Code.

5.13 Where test SMETS2+ SM WAN connection equipment is to be installed at a Testing Participant's premises, the Testing Participant shall for each connection to a testing environment:

(a) provide a suitably prepared area, with suitable power feeds prior to the installation of any equipment by the DCC, as specified by the DCC as part of the site survey ahead of an order being confirmed;

(b) provide suitable broadband connectivity or a phone connection as advised by the DCC following a site survey or analysis of the Testing Participant's requirements, over which a connection can be established to the data centre for the relevant Region and testing environment, as required, which enables transmission of data between the Testing Participant's test laboratory and the DCC;

(c) carry out routine inspection of the equipment supplied by the DCC and notify the DCC's Service Desk if there appears to be a problem with the equipment; and

(d) carry out maintenance of the environment in which the equipment is located.

5.14 Where the DCC is required to install any test SMETS2+ SM WAN connection equipment, the DCC shall take all reasonable steps to avoid interruption to existing services at those premises. Where existing services are interrupted, the DCC shall take all reasonable steps to minimise the length and impact of any interruption and shall ensure that existing services are restored as soon as reasonably practicable.

5.15 Where the DCC has acted in accordance with Good Industry Practice during installation, maintenance and / or removal activities, the DCC shall not be responsible for or liable to the Testing Participant for making good any minor repairs to decoration that have become necessary as a result of those activities.

5.16 The Testing Participant shall be entitled to and shall only use the connection to the test SMETS2+ SM WAN for the purposes of undertaking the tests set out in Section H14.1(c); Section H14.1(d); and Section H14.1(e), and shall not use it for any other purpose.

5.17 [NOT IN USE]

Fault Diagnosis, Maintenance and Removal of Test SMETS2+ SM WAN Connection Equipment

5.18 The DCC shall undertake the following in relation to the test SMETS2+ SM WAN connection:

(a) provide remote assistance to the Testing Participant to diagnose faults with any connection to the test SMETS2+ SM WAN, including faults with any test SM WAN connection equipment or environment supplied by the DCC;

(b) rectify any faults with the connection to the test SMETS2+ SM WAN, including faults with any test SMETS2+ SM WAN connection equipment supplied by the DCC. Where rectification requires replacement of equipment the DCC shall remove any redundant equipment within 30 days of replacement of the equipment. In the event that the DCC fails to remove the equipment within this period, the Testing Participant may dispose of the equipment and shall notify the DCC at least 5 days prior to disposing of the equipment, provided that the DCC shall have the right to remove the equipment prior to the end of that 5 day period;

(c) provide ongoing configuration management of test SMETS2+ SM WAN connection equipment;

(d) ensure that the equipment is operated and maintained in accordance with Good Industry Practice, and that it complies with all applicable Laws and Directives; and

(e) manage and implement firmware and hardware upgrades associated with the test SMETS2+ SM WAN connection equipment.

5.19 The DCC may modify or replace the equipment where necessary to maintain the operation of the test SMETS2+ SM WAN, provided that such modification or replacement does not materially diminish the performance of the test SMETS2+ SM WAN, and only after giving reasonable notice to the Party of the need to modify or replace the equipment.

5.20 The Testing Participant, at whose premises the test SMETS2+ SM WAN connection equipment is (or is to be) installed, shall provide the DCC with such access to that premises as the DCC may reasonably require in order to allow it to undertake the installation, maintenance or removal of the test SMETS2+ SM WAN connection equipment. The DCC shall ensure that all persons exercising such rights of access do so in compliance with the site rules and reasonable instructions of the Testing Participant.

5.21 Where the Testing Participant ceases to be a Party or notifies the DCC that it no longer requires the connection to the test SMETS2+ SM WAN (on not less than 1 month’s prior notice), then the DCC shall within 30 days of that notice period ending or that Testing Participant ceasing to be a Party, remove the test

SMETS2+ SM WAN connection equipment from the relevant premises in accordance with Good Industry Practice and all applicable Laws and Directives.

5.22 In the event that test SMETS2+ SM WAN connection equipment is not removed within 30 days, the Testing Participant may dispose of that equipment and shall notify the DCC at least 5 days prior to disposing of the test SMETS2+ SM WAN connection equipment, provided that the DCC shall have the right to remove the equipment prior to the end of that 5 day period.

6. Requirements for Use of DCC Test Labs

6.1 Pursuant to Section H14.9(a), the DCC shall make available the DCC's physical test laboratories to Testing Participants to conduct User Entry Process Tests, Device and User System Tests, Modification Proposal implementation testing, DCC Internal Systems change testing, Interoperability and Innovation Events and RF Noise Testing.

6.2 Where a Testing Participant is performing tests in a DCC physical test laboratory, it must comply with any reasonable supplemental terms and conditions that are required by the DCC and notified prior to testing which may include:

(a) identification and authorisation of the individual(s) requiring access to the DCC physical test laboratory;

(b) requirements to maintain confidentiality of information;

(c) policies relating to the acceptable use of the laboratory and equipment; and

(d) requirements to follow:

(i) health and safety guidance for test laboratories;

(ii) security guidance; and

(iii) training on use of test laboratories and installation of Devices in the spaces provided.

6.3 Where DCC considers that the Testing Participant has breached any SEC obligations relating to the use of a Testing Service at the physical test laboratory it shall notify the Testing Participant to that effect. The DCC and Testing Participant shall use reasonable steps to rectify the situation. Where DCC considers that the situation has not been rectified the DCC may request that the Testing Participant shall immediately remove its Devices from the Test Lab and the Testing Participant shall comply with such a request. DCC will provide the Testing Participant with:

(a) the reason(s) for this instruction; and

(b) the steps that must be taken and the evidence required, in order for the Participant to re-commence testing.

6.4 A Testing Participant may dispute the reasons for the instruction in clause a) or b) to the Panel and the DCC and Testing Participant shall comply with any determination.

6.5 Where a Testing Participant wishes to install their own Devices, in a DCC physical test laboratory, the Testing Participant must provide the following to the DCC prior to installing a Device in a DCC physical test laboratory:

(a) in the case of SMETS2+ Devices only, where a Testing Participant reasonably believes that Devices do not conform to SMETS2+ that any non-compliant aspects are notified to, and agreed with, the DCC (such agreement not to be unreasonably withheld). Supporting information should be provided, including evidence of testing that has been undertaken, which could include the use of GIT for Industry;

(b) evidence that all the supplied Devices are safe to store, install, operate and decommission. This may be in the form of a statement of compliance with the relevant parts of the CE marking or equivalent; and

(c) confirmation that the Devices have been produced in accordance with a recognised quality assurance process and a defined testing issue management and configuration management process.

6.6 Where a Testing Participant wishes to install their own Devices in a DCC physical test laboratory, the Testing Participant must:

(a) remove Devices from the DCC physical test laboratory by 17:00 on the last day of the allocated test slot; and

(b) comply with any other reasonable restrictions notified by the DCC, which the DCC shall notify to a Testing Participant when informing them that their requested test slot is available.

6.7 For the purpose of Section H14.10, storage space requirements for equipment shall be arranged between the DCC and the Testing Participant when making application to use the physical test laboratory. Pursuant to Section H14.10, the DCC will store at its physical test laboratories any number of Devices that a Testing Participant has procured itself that the DCC can reasonably accommodate.

6.8 In relation to testing being undertaken in a DCC physical test laboratory:

(a) without prejudice to the DCC's obligations under Section M4 (Confidentiality), each Testing Participant shall take reasonable steps to preserve the confidentiality of the Testing Participant's Confidential Information;

(b) no Testing Participant shall attempt to discover, overhear or obtain Data regarding testing being conducted by other Testing Participants in the DCC physical test laboratory; and

(c) (without prejudice to (b) above) no Testing Participant shall disclose or use any Data of the DCC or any other Testing Participant that the first Testing Participant discovers, overhears or obtains in the course of using the DCC's physical test laboratory.

7. User Entry Process Tests

7.1 In accordance with Section H14.9, DCC physical test laboratories will house sets of Devices for a Testing Participant undertaking User Entry Process Testing or Additional SR Testing, via UEPT process, or the DCC shall provide Test Stubs or emulators for SMETS2+ Devices, with a set consisting of:

(a) For tests in respect of SMETS2+ Devices, if this functionality is being tested:

(i) one Test Communications Hub;

(ii) one Electricity Smart Meter or one Electricity Smart Meter which supports Auxiliary Load Control;

(iii) one Gas Smart Meter;

(iv) one Standalone Auxiliary Proportional Controller; and

(v) one HAN Controlled Auxiliary Load Control Switch;

(b) For tests in respect of SMETS1 Devices, two sets of Devices comprising Device Model Combinations that are on the list of Eligible Product Combinations, comprising one of the following, if this functionality is being tested:

(i) a Communications Hub, an Electricity Smart Meter, a Gas Smart Meter and an IHD; or

(ii) a Communications Hub, an Electricity Smart Meter, a Gas Smart Meter and a SMETS1 PPMID.

7.2 DCC shall allocate a number of spaces in the DCC physical test laboratory, together with Device sets to the Testing Participant, if undertaking User Entry Process Testing or Additional SR Testing, via the UEPT process, as agreed at the initiation meeting, according to the following allocation schedule:

(a) Parties that are Affiliates undertaking testing in the User Roles of Import Supplier and / or Gas Supplier will collectively be allocated a total of two SMET2+ Device sets and two SMETS1 Device sets to undertake testing in those User Roles;

(b) Parties that are Affiliates undertaking testing in the User Role of Export Supplier will collectively be allocated a total of two SMETS2+ Device sets and two SMETS1 Device sets to undertake testing in that User Role;

(c) Parties that are Affiliates undertaking testing in the User Roles of Electricity Distributor and / or Gas Transporter will collectively be allocated a total of two SMETS2+ Device sets and two SMETS1 Device sets to undertake testing in those User Roles. Where Parties that are Affiliates hold Electricity Distribution Licences and/or Gas Transportation Licences in different Regions, in the case of SMETS2+ Device sets, such Affiliates shall be offered on request two Device sets collectively in relation to each Region; and

(d) Parties that are Affiliates undertaking testing in the User Role of Other User will collectively be allocated a total of two SMETS2+ Device sets and two SMETS1 Device sets to undertake testing in that User Role.

7.3 The Device sets allocated for the conduct of User Entry Process Tests or Additional SR Testing, via the UEPT process shall not be used for other testing without the agreement of DCC, such agreement not to be unreasonably withheld.

8. Device and User System Tests

8.1 Each Party is eligible to undertake Device and User System Tests once the following entry criteria have been achieved:

(a) for a Testing Participant conducting the user system element of Device and User System Testing:

confirmation from the DCC that the Testing Participant has successfully completed SREPT and UEPT for the User Role(s) that they intend to participate in when undertaking User System Testing.

(b) for a Testing Participant conducting the device testing element of Device and User System Testing, either:

(i) confirmation from the DCC that the Testing Participant has successfully completed SREPT and UEPT for the User Role(s) that they intend to participate in when undertaking Device Testing; or

(ii) if the Testing Participant is not eligible to conduct UEPT:

(A) demonstrate to the DCC that it is capable of sending Service Requests and receiving Service Responses in accordance with the DCC User Interface Specification by establishing a DCC Gateway Connection and performing a DUIS Connectivity Test, (as defined in the Common Test Scenarios Document); and

(B) provide evidence to the DCC that all Service Requests can be generated in accordance with the DCC User Interface Specification; the form of this evidence may include test results and will be agreed on an individual basis between the DCC and each Testing Participant.

8.2 Where agreement cannot be reached under clause 8.1, the Testing Participant may dispute the reasons for disagreement to the Panel under Section H14.16.

8.3 For the purpose of user system testing or Additional SR Testing via the Device and User System Testing (DUST) process, with SMETS2+ Devices, the DCC shall provide upon request Device(s), Test Stubs or Emulators, as provided for in Section H14.9. In respect of user system testing or Additional SR Testing via the Device and User System Testing (DUST) process with SMETS1 Devices, the DCC shall, at a minimum, provide Device Model Combinations upon request for use in a DCC laboratory that consists of two Device Model Combinations that are on the list of Eligible Product Combinations comprising one of each of the following:

(a) a SMETS1 Communication Hub, a SMETS1 Electricity Smart Meter, a SMETS1 Gas Smart Meter, and a SMETS1 IHD; and

(b) a SMETS1 Communication Hub, a SMETS1 Electricity Smart Meter, a SMETS1 Gas Smart Meter, and a SMETS1 PPMID.

Subject to Clause 8.3A, the DCC shall take all reasonable steps to provide all of the Device Model Combinations that are on the list of Eligible Product Combinations for use in testing, and to enable a Testing Participant to select the particular Device Model Combination(s) that it uses in testing, subject to the DCC being able to source the Device Model Combinations.

8.3A Where Migration DUST is no longer available pursuant to clause 17.24 of the MTAD (as described in Appendix AK) the DCC shall no longer be required to install new Devices pursuant to Clause 8.3 where those Devices are of Device Models that would, prior to the decommissioning of the associated Requesting Party, have been capable of being migrated from the SMETS1 SMSO associated with that Requesting Party. In circumstances where there are insufficient test devices available to fulfil concurrent demand for Testing Services, DCC may prioritise the provision of Devices to a Testing Participant for undertaking UEPT and will therefore be entitled to delay the provision of Device and User System Testing (DUST) to the Testing Participant that requires use of the same Devices. Where the DCC delays the provision of DUST to the Testing Participant it shall notify the Testing Participant that it is doing so due to the need to prioritise the use of Devices for UEPT. Where the Testing Participant disagrees with the DCC's decision to prioritise the use of Devices for UEPT, it may refer the matter to the Panel and the DCC and Testing Participant shall comply with any final determination of the Panel as to which Testing Service should be prioritised.

8.4 As set out in Section H14.10, a Testing Participant may supply its own Device(s) provided prior agreement has been obtained from the DCC and providing that the Device(s) complies with the following:

(a) the Device(s) can reasonably be accommodated in the space allocated;

(b) the Device(s) meet the criteria set out in clause 6.5, were they to be installed in a DCC physical test laboratory;

(c) In the case of SMETS1 Devices:

(i) the Device Model Combination is on the list of Eligible Product Combinations; and

(ii) Migration DUST is available pursuant to clause 17.24 of the MTAD (as described in Appendix AK):

(d) Unless otherwise agreed: each Testing Participant shall be responsible for ordering from the DCC the SMETS1 Communications Hubs, Test Communications Hubs and Smart Meters, IHDs, SMETS1 PPMIDs, Test Stubs or emulators for testing that it wishes the DCC to provide and installing them in the space allocated, as well as for their removal at the end of the testing slot; and

(e) any other physical interaction with the Devices shall be the responsibility of that Testing Participant and in accordance with any other reasonable instructions notified to the Testing Participant by the DCC.

8.5 The following alerts may be generated by SMETS2+ Devices or, as necessary, Test Stubs or emulators and Test Communications Hubs from within a DCC physical test laboratory:

(a) GSME – Low Battery Capacity (GBCS reference 0x8F1F)

(b) ESME / GSME Only: Trusted Source Authentication Failure (GBCS reference 0x8F3D)

(c) Supply Armed (GBCS reference 0x8F32);

(d) Polyphase ESME – Voltage Alert (GBCS reference 0x8005)

(e) Device Joined SMHAN (GBCS reference 0x8183);

(f) Average RMS Voltage above Average RMS Over Voltage Threshold (current value over threshold, previous value below threshold) (GBCS reference 0x8002);

(g) Future - date HAN Interface Command Successfully Actioned (GBCS reference 0x8F66);

(h) Supply Outage Restored (GBCS reference 0x8F35);

(i) Supply Outage Restored – Outage >= 3 minutes (GBCS reference 0x8F36);

(j) Device Identity Confirmation (DUIS reference N16);

(k) Schedule removal because of CoS (DUIS reference N17);

(l) Device CoS (DUIS reference N27); and

(m) PowerOutageEvent (DUIS reference AD1).

8.6 The DCC will support the generation of the following alerts, upon Test Participant request, in relation to SMETS1 Devices within a DCC physical test laboratory:

(a) Unauthorised Physical Access: Tamper Detect (SMETS1 Supporting Requirements reference 0x8F3F))

(b) Supply Armed (SMETS1 Supporting Requirements reference 0x8F32);

(c) SMETS1 Average RMS Voltage above Average RMS Over Voltage Threshold (SMETS1 Supporting Requirements reference 0x8F40);

(d) Device Identity Confirmation (DUIS reference N16);

(e) Schedule removal because of CoS (DUIS reference N17);

(f) Device CoS (DUIS reference N27);

(g) SMETS1 Service Provider Alert (DUIS reference N55); and

(h) SMETS1 Service Provider Provision of prepayment top-up UTRN (DUIS reference N56).

8.7 Additional alerts or response codes required may also be generated by the Testing Participant when using Smart Meters (including Electricity Smart Meters which support Auxiliary Load Control), SMETS1 Communications Hubs, Test Communications Hubs, HAN Controlled Auxiliary Load Control Switches and Standalone Auxiliary Proportional Controllers within a DCC physical test laboratory. However, further alerts may only be generated where they do not require physical interaction with the Devices or a change to the power supply in the DCC physical test laboratory, or where the DCC has given prior agreement and the actions comply with Health and Safety and any other reasonable instructions of the DCC.

8.8 When undertaking Device and User System Testing, the DCC and each Testing Participant shall take reasonable steps to comply with the timetables set out in Table 1 and Table 2 in clause 8, or another timetable reasonably agreed.

Table 1, below, sets out a high-level timetable for initiating testing. In the From and To columns, where an item is relevant to test laboratories, either “Remote Lab” or “DCC Lab” is shown, to clarify whether it relates to Testing Participants using Remote Test Labs or DCC physical test laboratories (or both).

Ref	By When	Action	From	To	Information / Action Required	Method
1a	See lead times described in the Guide for Testing Participants	Order equipment and DCCKI Test Certificate required to commence testing specifying which environment. Note a separate DCCKI Test Certificate will be required for	Testing Participant (Remote Lab)	DCC	This could include ordering • Remote SM WAN equipment to connect Remote Lab to CSP test system (SMETS2+ only) • DCC Gateway Connection • Test Communications Hubs (SMETS2 + only)	Via DCC Service Desk

		each test environment				
1b			Testing Participant (DCC Lab)	DCC	This could include ordering - DCC Gateway Connection	Via DCC Service Desk
2	See lead times agreed with Device manufacturer (or with DCC if Devices provided by DCC)	Order Devices required to commence testing, including supply of certificates	Testing Participant (Remote Lab + DCC Lab)	Meter Manufacture r (or DCC)	Order Devices	Via Meter Manufacturer or via DCC Service Desk
3	40 working days (or where less, as much prior notice as is reasonably practicable, as per H14.8) before Participant intends to commence testing[1]	Notify DCC of intention to commence testing specifying which environment. Subject to potential later constraints and agreement with DCC it may be possible to change the specified environment during the 40 Working Day period	Testing Participant (Remote Lab + DCC Lab)	DCC	Date to commence testing, whether testing to be conducted in DCC physical test laboratory (and which) or in remote test lab.	Email
4	30 Working Days before Participant intends to commence testing	Test Initiation Meeting	Testing Participants (Remote Lab + DCC Lab)	DCC	Entry criteria, as described in clause 8.1, evidenced. (Meeting offered to all TP's can be declined by TP's who are already testing in End to End)	Meeting

[1] This notification can be given before a Testing Participant completes UEPT. The Testing Participant may commence User System/Device Testing immediately upon completing UEPT, providing that 40 working days have elapsed since giving notice.

5	20 Working Days prior to the start of testing	Publish Schedule of available test slots in DCC physical test laboratories	DCC		Schedule – which will be maintained on an enduring basis	DCC SharePoint
6	15 Working Days prior to the start of Device and User System Testing	Health/safety & other CSP Lab training	DCC	Testing Participant (DCC Lab)	DCC to deliver training as described in clause 6.2. Method of training to be agreed.	As set out in Guide for Testing Participants
7	No later than 10 Working Days prior to the start of testing	Provide test tool to participant to record Testing Issues	DCC	Testing Participant (Remote Lab + DCC Lab)	Testing Issue Management Tool	
8	No later than 5 Working Days prior to the start of testing	Complete Readiness Verification	Testing Participant (Remote Lab + DCC Lab)	DCC	Completed Quality Gate Checklist, see section entitled 'Checklist' in Guide for Testing Participants.	Email
9	No later than 2 Working Days prior to the start of testing	Confirm criteria in Quality Gate Checklist met or request further preparatory work	DCC	Testing Participant (Remote Lab + DCC Lab)	Quality Gate Checklist If DCC requests further preparatory work, it may be necessary to release the test slot and reschedule the testing, and Testing Participant to repeat step 8.	Meeting
10a	1st Day of testing	Perform DUIS connectivity test, as defined in Common Test Scenarios Document, if necessary, and commence testing	Testing Participant (Remote Lab)		In accordance with terms and conditions provided by DCC.	
10b		Unless otherwise agreed install	Testing Participant (DCC Lab)			

		Devices, and commence Testing				
11	Last day of testing	Unless otherwise agreed uninstall Devices from DCC test laboratory	Testing Participant (DCC Lab)		Terms and conditions required by DCC	

Table 1 - Timetable for test initiation

Table 2, below, sets out the timetable to be followed by DCC and each Testing Participant on a monthly basis to enable scheduling of Testing Participants into a DCC physical test laboratory.

Ref	By When	Action	From	To	Information Required	Method
1	15th of each month (or previous working day)	Request test slot[2] specifying which environment	Testing Participant (CSP Lab)	DCC	Date of commencing test slot, number of meter Devices sets / DMCs to be tested which DMCs to be tested and duration of testing.	Email
2	First working day after 15th of each month	Publish test slot details	DCC	Testing Participant (CSP / DCC Lab)	Confirm that requested test slot is available (for slot commencing following month) or suggest alternative.	Email
3	Within 5 working days of DCC's publication of test slot	Confirm intention to use test slot in DCC physical test laboratory	Testing Participant (CSP Lab)	DCC		Email
4	Periodically, as required.	Update test schedule and republish	DCC	Testing Participants (CSP Lab)	Start and duration of test slot and number of spaces for Device sets	DCC SharePoint

[2] Note that test slots commence on the first working day of each month. Notice must be given by the 15th of a month (or the previous working day if 15th is not a working day), to obtain a slot commencing the following month.

Table 2 - Timetable for test slot scheduling

9. SMETS1 Pending Product Combinations Tests

9.1 A Testing Participant can request the DCC to execute SMETS1 Pending Product Combinations Tests (hereafter referred to as a "**PPCT**") to one or more combinations of SMETS1 Device Models (hereafter referred to as "**DMCs**") and communication services provider that are not at that time on the list of Eligible Product Combinations.

9.2 When requesting PPCT, the Testing Participant shall provide the DCC with all data pertaining to the DMC that is reasonably required and requested by the DCC, and shall indicate whether it is requesting that the processing of the DMC through PPCT is prioritised due to the DMC arising as a consequence of the need for a firmware upgrade that is required to address a material security vulnerability on an urgent basis. This data reasonably required by the DCC shall include (but is not limited to) Device Models, release notes, Device configuration, user guidance notes, and a nominated contact for the DCC to liaise with during testing for receipt of reports, and associated contact details. When a Testing Participant requests PPCT, subject to clause 9.3, the DCC shall enter the DMC on the list of Pending Product Combinations with a status of 'under assessment'.

9.3 Each Testing Participant that is requesting PPCT shall ensure that it has obtained consent from any relevant Manufacturer for its name to be published in the list of Pending Product Combinations or shall notify the DCC at the time that it is requesting the testing that such information should be treated as confidential in accordance with Section M4 of this Code. In the absence of such a notification, the DCC shall not be required to treat such information as confidential. Where the DCC is required to treat the information as confidential it shall not add the DMC to the list of Pending Product Combinations.

9.4 Following receipt of all of the data that the DCC reasonably requires and requested pursuant to clause 9.2, the DCC shall determine whether testing is required and shall notify the Testing Participant accordingly.

9.5 In determining whether or not testing is required, the DCC shall take into account the following:

(a) whether the DMC proposed for testing is on the list of SMETS1 Eligible Product Combinations; and

(b) whether the DMC proposed is substantively equivalent to an existing DMC that is on the list of SMETS1 Eligible Product Combinations.

9.6 Where the DMC proposed for testing is on the list of SMETS1 Eligible Product Combinations or where, in the DCC's opinion the DMC proposed for testing is substantively equivalent to a DMC that is on the list of SMETS1 Eligible Product Combinations, the DCC shall notify the Testing Participant accordingly and PPCT shall be deemed to have been successfully completed for the purposes of this Code. The DCC shall:

(a) where the DCC is of the opinion that the DMC proposed for testing is substantively equivalent to a DMC that is on the list of SMETS1 Eligible Product Combinations, ensure that it documents within its organisation its evidence and/or rationale to support this position;

(b) provide a PPCT completion certificate to the Testing Participant; and

b) subject to clause 9.3, update the list of Pending Product Combinations to reflect the DMC testing status as 'completed' and indicating that the DMC has been entered on the list of SMETS1 Eligible Product Combinations.

9.6A Following expiry of the RP Decommissioning Date for a Requesting Party (pursuant to Clause 7 of Appendix AL) the DCC shall no longer be required to install new Devices in its test laboratory where those Devices are of Device Models that would only, prior to the decommissioning of the associated Requesting Party, have been capable of being migrated from the SMETS1 SMSO associated with that Requesting Party.

9.6B The DCC shall not be required to complete PPCT for a DMC where:

(a) the RP Decommissioning Date for the Requesting Party associated with the SMETS1 SMSO from whom the new DMC would only have been capable of being migrated has expired (pursuant to Clause 7 of Appendix AL);

(b) DCC determines that the new DMC is not substantively equivalent to a DMC that is on the list of SMETS1 Eligible Product Combinations and testing within PPCT is required for the proposed Device Model Combination; and

(c) DCC has no existing device(s) in the DCC test laboratory that can be firmware upgraded to align with the proposed new Device Model(s) and used for testing.

The DCC shall promptly notify the Testing Party where it cannot complete PPCT and copy any such notification to the Authority and the Secretary of State.

9.7 Where the DCC determines that testing is required, the DCC shall notify the Testing Participant and shall state whether the Testing Participant is required to provide DCC with two sets of the DMC for testing. Following receipt of the DCC’s notice, the Testing Participant shall provide the DCC with:

(a) their proposed start date for testing; and

(b) where the testing participant is required to provide two sets of the DMC for testing, the date on which they will provide the DCC with two sets of the DMC to be installed by the DCC for testing.

The proposed start date for testing shall be at least 25 Working Days after the date on which the Testing Participant informs the DCC of its proposed date. The date on which the Testing Participant shall provide the DMCs to the DCC for PPCT shall be at least 5 Working Days prior to the Testing Participant’s proposed start date for testing.

9.8 Following the receipt of the proposed start date for testing, the DCC shall provide confirmation to the Testing Participant of the start date and the date on which the DMCs will be provided to the DCC (except where the proposed dates do not meet the minimum notice periods set out in clause 9.7 in which case the DCC shall ask the Testing Participant to re-submit their proposed dates). In doing so the DCC shall take all reasonable steps to accommodate the two dates set out in clause 9.7, where this is not possible the DCC shall select start dates that are as soon as reasonably practicable thereafter.

9.9 Following receipt of the DMC device sets from the Testing Participant, the DCC shall install the component Devices that make up the DMC in the DCC test laboratory, in order to facilitate the commencement of testing on the agreed start date.

9.10 The DCC shall take all reasonable steps to commence the tests on the start date and complete them as soon as is reasonably practicable. Where:

(a) the DCC is unable to commence the tests on the start date; or

(b) where the Testing Participant is unable to provide the DMC device sets by the agreed planned date,

the DCC shall discuss with the Testing Participant and shall notify a revised date(s), which shall be the earliest available date(s) in the DCC's testing schedule.

9.11 Upon successful completion of testing of the DMC the DCC shall:

(a) provide a PPCT completion certificate to the Testing Participant;

(b) return the test devices provided to the DCC to the Testing Participant; and

(c) subject to clause 9.3, update the list of Pending Product Combinations to reflect the DMC testing status as 'completed' and indicating that the DMC has been moved to the list of SMETS1 Eligible Product Combinations.

9.12 Where testing has not successfully completed, the DCC shall:

(a) inform the Testing Participant in a summary report which sets out:

(i) the reason(s) why the DMC testing has been suspended as either:

(A) change is required to the DMC to enable successful completion of testing; or

(B) a material change to the DCC Systems and/or modification to this Code need to be made in respect of the combination of SMETS1 Device Models to enable successful completion of testing.

(ii) the details of all test results which are not an expected outcome, and:

(A) where a Testing Participant has provided a production device for testing, the DCC shall provide a report which shall contain logging of the traffic on the DCC systems;

(B) where a Testing Participant has provided devices capable of revealing the Zigbee and network link keys, the DCC shall provide a report which shall contain logging of the traffic on the DCC systems and Zigbee logs of HAN traffic; and

(b) subject to clause 9.3, update the list of Pending Product Combinations to reflect the DMC's testing status as 'suspended'.

9.13 Where the information provided by the DCC pursuant to Clause 9.12 indicates that the inability to successfully complete testing arose as a consequence of an issue(s) with the Device(s) provided for testing, a Testing Participant may submit a revised DMC for testing once the issue(s) has been resolved. In so doing, the Testing Participant shall provide a release note that confirms that the appropriate fixes have been applied and tested successfully, and shall follow the process for requesting PPCT as set out in this Clause 9. The DCC shall then update the list of Pending Product Combinations to reflect the testing status of the original DMC as 'withdrawn'.

9.14 Where the information provided by the DCC pursuant to Clause 9.12 (i) (B) indicated that that in order for testing to successfully complete, a material change was required to the DCC Total System or a SEC Modification was required, the Testing Participant shall be entitled to resubmit the DMC for testing where the required change or Modification has been made and where it wishes to resubmit shall follow the process for requesting PPCT set out in this Clause 9.

SMETS1 Pending Product Combinations Tests: Fast Track Process

9.15 Where, for a firmware upgrade required to address a material security vulnerability, a Testing Participant requests that the processing of a DMC through PPCT is prioritised in order to achieve their proposed rectification date for the vulnerability, the DCC shall contact the Code Administrator to confirm that the security vulnerability has been notified to the Security Sub-Committee in accordance with Section G3.18(c) of the Code. The DCC shall also inform the Code Administrator of when (subject to Clause 9.10) processing of the DMC through PPCT would complete if it is not prioritised and, if the proposed rectification date of the vulnerability is earlier than this date, when it would be expected to complete if it is prioritised.

9.16 The Code Administrator, on behalf of the Security Sub-Committee, shall confirm to the DCC whether:

(a) the vulnerability has been reported to the Security Sub-Committee;

(b) the Security Sub-Committee Chair considers the vulnerability to be material; and

(c) whether the Security Sub-Committee Chair considers that the materiality of the vulnerability warrants the processing of the resultant DMC through PPCT on an urgent basis.

9.17 Where, pursuant to Clause 9.16, it is confirmed that the Security Sub-Committee considers that the DMC should be processed through PPCT on an urgent basis, then the DCC shall so prioritise the processing of the DMC. Where this (despite the DCC taking reasonable steps to avoid this being the case) results in previously notified commencement dates for the testing of other DMCs in PPCT needing to change, the DCC shall notify the affected Testing Participant(s). In determining the revised dates, the DCC shall, where reasonably practicable, take any affected Testing Participant's views of those dates into account.

10. DCC Internal System Change Testing

10.1 The DCC shall publish a plan notifying changes to the DCC Internal Systems which includes a reasonable period for Parties and/or RDPs to be involved in any testing of the change to the DCC Internal Systems prior to its implementation, as provided for in Section H8.8(c).

10.2 DCC shall provide Parties and/or RDPs the opportunity to conduct testing of the change to the DCC Internal System remotely and / or in DCC physical test laboratories.

10.3 DCC and each Party or RDP wishing to conduct testing of changes to DCC Internal Systems shall take reasonable steps to comply with the timetables set out in Table 1 and Table 2 in clause 8 where required the type of testing being performed, unless determined otherwise in accordance with the DCC Release Management Policy.

11. Modification Proposal Implementation Testing

11.1 Where the Panel determines, pursuant to Section H14.35, persons eligible to undertake implementation testing for a Modification Proposal, the DCC shall facilitate their participation remotely and / or using DCC physical test laboratories, unless determined otherwise by the Panel.

12. Use of Testing Issue Management Tool

12.1 Where DCC makes available a Testing Issue Management Tool to a Testing Participant and the Testing Participant elects to use such tool, the DCC and each Testing Participant shall comply with all reasonable terms set out by the DCC relating to the use of the Testing Issue Management Tool.

12.2 The DCC shall notify any terms relating to the use of the Testing Issue Management Tool to each Testing Participant prior to use of the Testing Issue Management Tool in support of any period of testing by a Testing Participant.

12.3 The Testing Issue Management Tool terms may include, without limitation:

(a) operational security;

(b) authentication and access control;

(c) boundary protection and interfaces;

(d) protecting data at rest and in transit;

(e) user and administrator separation of data;

(f) information relating to permitted users; and

(g) testing security.

13. Other Obligations

13.1 The DCC shall ensure that, where requested by a Testing Participant, it provides reasonable assistance and support to that Testing Participant in resolving testing issues. In support of the activities detailed in this document the DCC Service Providers shall provide support which shall include inter alia:

(a) the installation and removal of SMETS1 Device Model Combinations (including SMETS1 IHDs) from DCC test laboratories;

(b) capturing and analysis of logs for test issue resolution; and

(c) representation on calls for a Testing Participant's test planning.

13.2 The DCC shall be accountable and responsible for the following deliverables in support of the test activities detailed in this document:

(a) general administration

(b) DCC test infrastructure and environments;

(c) DCC test laboratory premises

13.3 Parties shall be accountable and responsible for their test infrastructure and their environments.

13.4 The DCC shall:

(a) notify Parties of outages and other matters affecting their testing; and

(b) support Parties undertaking the test activities detailed in this document.

13.5 The DCC systems integrator shall:

(a) support Parties undertaking of the test activities detailed in this document

(b) provide test execution and environment usage schedules;

(c) administer the testing issue resolution process and provide the testing issue management tool; and

(d) operate the master configuration management plan.

13.6 The DCC DSP shall:

(a) provide the DSP component of the relevant test environment and related data;

(b) provide support for DSP solution elements and DSP component of the relevant test environment;

(c) provide fixes required in DSP solution elements; and

(d) provide resource to support Parties undertaking testing.

13.7 Other DCC Service Providers shall:

(a) provide relevant components of or connections to the relevant test environment and related data;

(b) provide support for relevant solution elements and components of the relevant test environment;

(c) provide fixes required in relevant solution elements;

(d) provide resource to support Parties undertaking testing;

(e) provide support to the DCC Systems Integrator in assisting in the administration of testing; and

(f) provide resource to triage and fix Testing Issues.

13.8 The DCC shall take all reasonable steps to maximise the reuse of any test Devices that are SMETS1 test Devices in its test laboratories and shall take all reasonable steps to ensure that such test Devices are used in accordance with Good Industry Practice.

14. Radio Frequency Noise Testing

14.1 RF Noise Testing shall be undertaken to the requirements as set out in the current Intimate Communications Hub Interface Specification (ICHIS) and the associated ICHIS Test Specification published on the DCC Website.

14.2 The DCC shall provide a reasonable number of each Communications Hub Antenna Structure (CHAS) test device listed in the current ICHIS to Testing Participants for the purposes of RF Noise Testing.

14.3 RF Noise Testing shall also provide the ability for the DCC to test new CHAS test devices not yet listed in the current ICHIS with SMETS2+ ESME and Communications Hub Hot Shoe Devices upon agreement with the relevant Testing Participant.

14.4 Where a Testing Participant requests RF Noise Testing, the DCC shall provide confirmation that it can accommodate the request and a quotation for the Charges associated with the service.

14.5 Where a Testing Participant wishes to accept the quotation for RF Noise Testing, the Testing Participant shall notify the DCC.

14.6 Where RF Noise Testing is undertaken at the DCC Test Labs then Section 6 will apply.

15. Interoperability and Innovation Events

15.1 Testing Participants will be notified of the schedule of events and issued invitations to attend by the DCC. Invitations to attend shall be issued via e-mail at least one month prior to the event.

15.2 The DCC shall notify any terms relating to the attendance of Interoperability and Innovation Events to each Testing Participant prior to the attendance of such an event.

15.3 Where an Interoperability and Innovation Event is held at the DCC Test Labs then Section 6 will apply.

15.4 No certification or accreditation is provided by attending these events.

16. GFI Testing

16.1 The DCC shall develop and make available via the DCC Website a policy describing the provisions and allocation requirements for types of GFI Testing.

16.2 The Testing Participant shall request GFI Testing Tools in accordance with the GFI Testing Policy.

16.3 Where a Testing Participant requests GFI Testing outside of the provisions and allocation requirements set out in the GFI Testing Policy, the DCC shall provide confirmation that it can accommodate the request and a quotation for the Charges of the service.

16.4 Where a Testing Participant wishes to accept the quotation for GFI Testing, the Testing Participant shall notify the DCC.

17. Wired Instrumented Test Communications Hub (ITCH)

17.1 The DCC shall make available to Testing Participants Dual Band SMETS2+ Instrumented Test Communication Hubs (ITCHs) which are a Communications Hub (CH) variant in which the SM-WAN interface is disabled. The Wired ITCH will contain the capability to be connected to a test environment Personal Computer (PC) via a wired interface. This will enable a Testing Participant to exchange messages, responses and alerts between the PC and the CH without the use of a WAN network.

17.2 Testing Participants may order Wired ITCHs in accordance with SEC Section F10.

Definitions & Interpretation

Communications Hub Antenna Structure (CHAS)	means a unit which is used for testing against the Intimate Communications Hub Interface Specification (ICHIS) Test Specification.
GIT for Industry	means a test tool provided by DCC to validate implementation of GBCS by a Device.
Quality Gate Checklist	means a checklist document used to support assessment whether criteria have been met.
Testing Issue Management Tool	means a test management tool that has the ability to log and track Testing Issues.
Testing Participants	means, in respect of each Testing Service, the persons (whether or not they are Parties) who are entitled to undertake such tests, as described in Section H14 (Testing Services).

18. DCC Boxed

18.1 The DCC shall develop and make available via the DCC Website a policy describing the provisions and allocation requirements for types of DCC Boxed.

18.2 The Testing Participants shall request DCC Boxed in accordance with such policy, and the DCC shall comply with such policy.

Version K 4.0

Appendix K

SMKI and Repository Test Scenarios Document

1. Introduction

1.1. Purpose

The purpose of this document is to:

- define the procedural steps to be undertaken by a Party or RDP wishing to complete the SMKI and Repository Entry Process Tests (SREPT). Section H14.23 requires those tests to be undertaken in accordance with this SMKI and Repository Test Scenarios Document;
- set out the SMKI and Repository Entry Process Tests that a Relevant Party or RDP must successfully complete in order to be entitled to apply to become an Authorised Subscriber or access the SMKI Repository in accordance with Section L7.1; and
- describe the role and responsibilities with regard to the conduct of SREPT including:
  - entry and exit requirements;
  - defining Test Scripts;
  - defining Test Data;
  - planning the manner in which tests will be undertaken;
  - executing the tests;
  - reporting the results of those tests to the DCC for approval; and
  - performing regression testing where required.

2. Scope

Section 5 of this document sets out which Test Scenarios a Relevant Party or RDP must successfully complete, depending upon:

- which SMKI interfaces or SMKI Repository Interface the Relevant Party or RDP will access and whether this is for Device Certificates or Organisation Certificates; and
- whether access to the SMKI interfaces will be through a DCC Gateway Connection or using the SMKI Portal interface via the Internet.

Section 8 Appendix C: Test Scenarios of this document sets out the SMKI and Repository Entry Process Test Scenarios as referred to in Section H14.22.

3. Test Preparation

The Enduring Testing Approach Document sets out rights and obligations relating to gaining Test Certificates.

Parties or RDPs wishing to undertake SREPT must comply with the security requirements applicable to Testing Participants set out in the Enduring Testing Approach Document.

To gain access to the test systems to undertake SREPT, as set out in the Enduring Testing Approach Document, the following activities must take place:

- the applicant organisation must have completed the procedure to verify the organisational identity for testing purposes;
- an applicant organisation must have at least one test SMKI Senior Responsible Officer (SMKI SRO) appointed for test purposes;
- an applicant organisation must have at least one test SMKI Authorised Responsible Officer (SMKI ARO) appointed for test purposes; and
- the procedure for provision of test credentials to SMKI AROs for accessing test SMKI Services and/or the test SMKI Repository Service must have been completed.

4. Test Sequence

A Relevant Party or RDP may undertake the Test Scenarios set out in this document in any order.

5. SREPT Procedure

5.1. Overview

This section describes the procedure that must be completed in order for a Relevant Party or RDP to complete SREPT.

5.2. SMKI & Repository Entry Process Testing

The matrices in Table 1 SREPT Matrix – DCC – DCC Gateway Connection and Table 2 SREPT Matrix – No DCC Gateway Connection, below, provide a mapping to determine which Test Scenarios described in this document a Relevant Party or RDP must undertake. The column 'SMKI RAPP Ref' is used to determine which tests should be performed, based on the interfaces the Relevant Party or RDP wishes to use to access the SMKI Services and/or SMKI Repository Services and whether they wish to subscribe for Organisation Certificates and/or Device Certificates.

Detailed Test Scenarios identified to support the SREPT process are listed in section 8.1 'SMKI and Repository Entry Process Test Scenarios with DCC Gateway Connection' and section 8.2 'SMKI & Repository Entry Process Test Scenarios without DCC Gateway Connection'.

5.2.1 Test Scenarios for Parties or RDPs with a DCC Gateway Connection

		Applicant Organisation				
Test Scenario Reference	Test Scenario Title	DCC (DCC Service Provider)	Supplier	RDP	Non-Supplier Party	SMKI RAP Ref
SMKI 02	Access the test SMKI Service, through the SMKI Portal interface over a DCC Gateway Connection	✓	✓	✓	✓	5.4.1 5.4.2
SMKI 03	Access the test SMKI Service, through the Ad Hoc Device CSR Web Service interface and the Batched Device CSR Web Service interface, over a DCC Gateway Connection	✓	✓		✓*	5.4.3 5.4.4
SMKI 05	Access the test SMKI Repository through the SMKI Repository Portal interface over a DCC Gateway Connection	✓	✓	✓	✓	5.4.5
SMKI 06	Access the test SMKI Repository via the SMKI Repository Web Service interface over a DCC Gateway Connection	✓	✓	✓	✓	5.4.6
SMKI 07	Access the test SMKI Repository through the SSH File Transfer Protocol (SFTP) interface over a DCC Gateway Connection	✓	✓	✓	✓	5.4.7
SMKI 22	Submit Organisation Certificate Signing Requests and receive the resulting Organisation Certificates, through the SMKI Portal interface over a DCC Gateway Connection	✓	✓	✓	✓	5.4.1
SMKI 23	Submit a Device Certificate Signing Request and receive the resulting Device Certificate through the SMKI Portal interface over a DCC Gateway Connection	✓	✓		✓*	5.4.2
SMKI 24	Submit a Batched Certificate Signing Request and receive Device Certificates through the SMKI Portal interface over a DCC Gateway Connection	✓	✓		✓*	5.4.2

SMKI 25	Submit a Device Certificate Signing Request and receive the resulting Device Certificate through the Ad Hoc Device CSR Web Service interface over a DCC Gateway Connection	✓	✓			5.4.3
SMKI 29	Download a copy of all 'In Use' SMKI Test Certificates from the test SMKI Repository through the SFTP (SSH File Transfer Protocol) interface over a DCC Gateway Connection	✓	✓	✓	✓	5.4.7
SMKI 30	Download a daily delta file of SMKI Test Certificates through the SFTP interface over a DCC Gateway Connection	✓	✓	✓	✓	5.4.7
SMKI 31	Query the test SMKI Repository for Organisation Certificates through the SMKI Repository Portal interface over a DCC Gateway Connection	✓	✓	✓	✓	5.4.5
SMKI 32	Query the test SMKI Repository for Organisation Certificates through the SMKI Repository Web Service interface over a DCC Gateway Connection	✓	✓	✓	✓	5.4.6
SMKI 33	Query the test SMKI Repository for Device Certificates through the SMKI Repository Portal interface over a DCC Gateway Connection	✓	✓		✓	5.4.5
SMKI 34	Query test SMKI Repository for Device Certificates through the SMKI Repository Web Service interface over a DCC Gateway Connection	✓	✓		✓	5.4.6
SMKI 48	Obtain the latest Organisation CRL and Organisation ARL through the SMKI Repository Portal interface over a DCC Gateway Connection	✓	✓	✓	✓	5.4.5
SMKI 50	Obtain the latest Organisation CRL and Organisation ARL through the SMKI Repository Web Service interface over a DCC Gateway Connection	✓	✓	✓	✓	5.4.6
SMKI 57	Submit a Batched Device Certificate Signing Request and receive Certificates for Devices through the Batched Device CSR Web Service interface over a DCC Gateway Connection	✓	✓		✓*	5.4.4

Table 1 SREPT Matrix – DCC Gateway Connection

Key

✓	Applicant organisation required to undertake this test if they wish to receive credentials for this service / access to this interface

✓* Applicant organisation required to undertake this test if they wish to access to this interface and can provide reasonable evidence to suggest that it is necessary for the applicant organisation to become an Authorised Subscriber for Device Certificates in order for them to carry out business processes that will, or are likely to, lead to the installation of Devices in premises

5.2.2 Test Scenarios for Parties without a DCC Gateway Connection

		Applicant Organisations		
SMKI SRTSD Scenario Reference	Headline Scenario Title	Supplier	Non-Supplier Party	SMKI RAPP Ref
SMKI 04	Access the test SMKI Services for (i) Organisation Certificates through the SMKI Portal interface over the internet	✓ ✓	✓ ✓*	5.4.1, 5.4.2
SMKI 08	Submit Requests for Repository content using the SMKI Portal interface over the internet	✓ ✓	✓ ✓*	5.4.1, 5.4.2
SMKI 26	Submit an Organisation Certificate Signing Request and receive the resulting Organisation Certificate through the SMKI Portal interface over the internet	✓	✓	5.4.1
SMKI 38	Download Organisation Certificates and OCA Certificates through the SMKI Portal interface over the internet	✓ ✓	✓* ✓	5.4.1, 5.4.2

Table 2 SREPT Matrix – No DCC Gateway Connection

Key

✓ Applicant organisation required to undertake this test if they wish to receive credentials for this service / access to this interface

✓* Applicant organisation required to undertake this test if they wish to access this interface and can provide reasonable evidence to suggest that it is necessary for the applicant organisation to become an Authorised Subscriber for Device Certificates in order for them to carry out business processes that will, or are likely to, lead to the installation of Devices in premises.

5.3. SREPT Initiation

Each Relevant Party or RDP and the DCC shall each take reasonable steps to comply with the timescales that are set out within the procedures in Table 3, Table 4 & Table 5. In the event that a Relevant Party or RDP does not comply with the timescales in Table 3, Table 4 & Table 5, the DCC will reschedule subsequent activities to occur as soon as is reasonably practicable thereafter and for such purposes the DCC may reschedule that Relevant Party or RDP's test execution date.

5.3.1 Procedural Steps

The table below sets out the steps that must be undertaken prior to initiation of the SREPT by both the DCC and the Relevant Party seeking to undertake SREPT and the timeframes within which such steps must be completed.

Ref	When	Action	From	To	Information Required	Method
5.3.1.1	60 Working Days (WD) prior to commencement of SREPT	Notify intention to undertake SREPT	Relevant Party or RDP	DCC	Party / RDP notification of intention to undertake testing • Party / RDP id (s) • Confirmation that notification provided to SECAS, User Role(s) • Test start date • Identity of Test Manager and contact details	By email as attachments
5.3.1.2	Within 2 WD of receipt of the notification under 5.3.1.1	Acknowledge request	DCC	Relevant Party or RDP	Confirmation of Party / RDP notification: • Party / RDP id (s) • Test start date • DCC Test Manager contact • Date for SREPT initiation meeting	By email as attachments
5.3.1.3	Within 5 WD of receipt of the notification under 5.3.1.2	Conduct SREPT initiation meeting	DCC	Relevant Party or RDP	DCC to provide guidance information on conducting SREPT including a guide to the SMKI and Repository Entry Process Tests.	Meeting

5.3.1.4	In each week occurring within the period from 40 WD prior to start of testing	Provide progress report, demonstrating readiness to begin tests	Relevant Party or RDP	DCC	Test Readiness Report	By email as attachments
5.3.1.5	25 WD prior to start of testing	Provide test artefacts to support conduct of SREPT	Relevant Party or RDP	DCC	• Test Plan incorporating the Test Schedule • Requirements Traceability Matrix (see section 6.1.6) • Test Scripts (see section 6.1.7) • Test Data Plan (see section 7)	By email as attachments
5.3.1.6	By 20 WD prior to start of testing	DCC complete review of test artefacts	DCC	Relevant Party or RDP	Details regarding any deficiencies in the test artefacts and where necessary, a revised start date for testing provided – continue from 5.3.1.7 Or, confirmation that the DCC has accepted the test artefacts – continue from 5.3.1.9	By email as attachments
5.3.1.7	By 10 WD prior to start of testing	Party / RDP to provide revised documents	Relevant Party or RDP	DCC	Revised documents	By email as attachments
5.3.1.8	By 7 WD prior to start of testing	DCC complete review of revised test artefacts	DCC	Relevant Party or RDP	Details regarding any deficiencies in the test artefacts and a revised start date for testing provided where agreed it is necessary – Regress and continue from 5.3.1.7 Or confirmation that test	By email as attachments

					artefacts accepted – continue from 5.3.1.9	
5.3.1.9	By 5 WD prior to start of testing	1. Review Test Readiness Report and confirm the Entry Criteria for commencing testing in relation to Relevant Party or RDP have been met 2. Confirm Start Date and Test Schedule for execution of tests by Relevant Party or RDP	DCC Quality Gate meeting	Relevant Party or RDP	Source: Test Readiness Report, Test Schedule Output: Confirmation of Relevant Party or RDP readiness to proceed	Quality Gate Review meeting
	If there is any outstanding documentation presented at the Quality Gate Review, the DCC shall assess it as part of its assessment of the Entry Criteria under clause 5.3.2					

Table 3 SREPT Initiation: Procedural Steps

5.3.2 SREPT Entry Criteria

Each Relevant Party or RDP wishing to undertake SREPT must comply with (and, where specified below, shall provide evidence of complying with) the following criteria prior to entry into SREPT:

- the interfaces that the Relevant Party or RDP wishes to access must have been identified to determine the SMKI & Repository Entry Process Tests that are to be undertaken;
- all relevant test artefacts (as set out in sections 5.3.1.1, 5.3.1.4 and 5.3.1.5) must have been produced by the Relevant Party or RDP and accepted by the DCC. This includes:
  - Party / RDP Notification of Intention to Undertake Testing
  - Test Readiness Report
  - Test Plan incorporating the Test Schedule

  - Requirements Traceability Matrix
  - Test Scripts
  - Test Data Plan
- have provided evidence that an appropriate test environment and an appropriate level of resources available to support the SREPT process; and
- confirm that the security requirements set out in the Enduring Testing Approach Document have been met.

Where the DCC reasonably believes that the Relevant Party or RDP has not met the Entry Criteria, the DCC may:

- prevent the Relevant Party or RDP from undertaking SREPT until such time as the DCC reasonably believes that the Relevant Party or RDP meets the Entry Criteria (and in which case DCC shall inform the Relevant Party or RDP why it believes that they have not met the Entry Criteria); and
- reschedule the test start date for the Relevant Party or RDP. In doing so, the DCC shall provide the earliest practicable alternative date; or
- provide provisional approval of the Test Readiness Report (and approval to proceed) with an understanding that the outstanding documentation will be provided before the start of testing, otherwise testing will not commence.

Pursuant to Section H14.25, where the DCC does not reasonably believe that a Relevant Party or RDP meets the Entry Criteria to commence testing, the Relevant Party or RDP may refer the matter to the Panel. Where the Panel determines that the Relevant Party or RDP has met the Entry Criteria, the DCC shall schedule the start of testing as soon as reasonably practicable thereafter.

5.4. SREPT Execution

5.4.1 Procedural Steps

The table below sets out the steps that must be undertaken prior to or during test execution by either the DCC or a Relevant Party or RDP seeking to undertake SREPT and the timeframes within which such steps must be complete as set out in the Test Schedule which will be updated by the Relevant Party or RDP from time to time to reflect test progress.

Ref	When	Action	From	To	Information Required	Method
5.4.1.1	SREPT Start Date or earlier (if appropriate)	Verification of Organisation Identity and appointment of, SMKI SRO and SMKI ARO	Relevant Party or RDP	DCC	Submission of relevant forms	As per Enduring Testing Approach Document

		for test purposes				
5.4.1.2	SREPT Start Date or earlier (if appropriate)	Carry out checks such that the Relevant Party or RDP has at least one test SMKI SRO and at least one test SMKI ARO. Confirm with Relevant Party or RDP.	DCC	Relevant Party or RDP	Confirm Organisation Identity is verified and test SMKI ARO and test SMKI SRO Registration is complete. Grant approval to execute SREPT scenarios and which scenarios will be undertaken	As per Enduring Testing Approach Document
5.4.1.3	In accordance with Test Schedule and 5.4.1.2 completed	Conduct SREPT	Relevant Party or RDP		Approved test artefacts	As per test artefacts
5.4.1.4	Daily Basis, or alternative schedule agreed with DCC	Provide daily progress report using the template provided to DCC	Relevant Party or RDP	DCC	Test execution dashboard and Daily Testing Issue Report	By email as attachment
5.4.1.5	SREPT execution complete	Provide Test Completion report	Relevant Party or RDP	DCC	SREPT completion report including: details of Test Scripts executed and Testing Issues resolved (see section 9.6)	By email as attachment

Table 4 SREPT Execution: Procedural Steps

5.4.2 SREPT Test Suspension/Resumption

During the execution of tests the DCC, Relevant Party or RDP each have the right to suspend testing where it reasonably considers that this is necessary.

Testing will only recommence when agreed by both the DCC and the Relevant Party or RDP subject to the suspension.

5.4.2.1 Possible Suspension Criteria

Reasonable grounds for suspension of testing may include any of the following;

- application components are not available as scheduled;
- a Testing Issue prevents further useful testing from proceeding;
- a significant percentage of planned Test Scripts for a given day fail, taking Testing Issue severity and volume of tests into consideration which would generate root cause analysis to be undertaken to establish the cause. Testing Issues trending should also be used to determine any recommendation. The outcome of any root cause analysis activity may result in testing being suspended;
- Test Scripts to be executed are in a "blocked" status due to an identified Testing Issue; and
- the Relevant Party or RDP has failed to comply with the procedural steps for executing SREPT.

5.4.2.2 Test Resumption Criteria

Where testing has been suspended, either the DCC or the Relevant Party or RDP as appropriate shall produce a test suspension report reflecting the cause of the suspension, and what actions are to be taken by whom and when in order for testing to resume – the 'Test Resumption Criteria'. The DCC and the Relevant Party or RDP shall take reasonable steps to support each other to achieve the Test Resumption Criteria.

Testing will only resume once the DCC or Relevant Party or RDP has demonstrated to the other Party's satisfaction that the Test Resumption Criteria have been met.

5.4.2.3 Disputes regarding Test Suspension/Resumption

Each of the DCC and the Party or RDP undertaking the SMKI and Repository Entry Process Tests may suspend testing in accordance with the requirements set out above. Any dispute between the DCC and a Party or the RDP regarding the suspension (or consequent resumption) of such testing may be referred to the Panel for its determination. Where the DCC or the Party or RDP disagrees with any such determination of the Panel, then the DCC or the Party or RDP may refer the matter to the Authority for its determination (which determination shall be final and binding for the purposes of this Code).

Where a dispute regarding the suspension/resumption of testing is made, testing will not resume whilst the dispute is being heard by the Panel, and/or until the Test Resumption Criteria are met by the DCC or the Relevant Party or RDP.

5.5. SREPT Completion

5.5.1 Procedural Steps

The table below sets out the steps that must be undertaken during test completion by either the DCC or Relevant Party or RDP and the timeframes within which such steps must be complete.

Ref	When	Action	From	To	Information Required	Method
5.5.1.1	Within 2 WD of receipt of the report in 5.4.1.5	Confirm receipt of notification of test complete (Test completion report)	DCC	Relevant Party or RDP	Test Completion Report (see section 9.6)	By email
5.5.1.2	Within 5 WD of receipt of the notification 5.5.1.1	DCC review completion report and confirm that SREPT concluded or further testing required	DCC	Relevant Party or RDP	Test Completion Report and evidence as requested by DCC. 5.4.1.5 refers	Quality Gate Review meeting
5.5.1.3	Within 2 WD of successful Quality Gate Review meeting	Confirm Test Complete	DCC	Relevant Party or RDP, SMKI Registration Authority	Issue Test Completion Certificate (see section 10) and provide copy to Registration Authority	By email as attachment

Table 5 SREPT Completion: Procedural Steps

Notwithstanding 5.5.1.3 above pursuant to Section H14.28 the DCC shall confirm on request by the Relevant Party or RDP whether or not it considers that the Relevant Party or RDP has successfully completed SREPT.

5.5.2 SREPT Exit Criteria

A Relevant Party or RDP must meet the following Exit Criteria prior to that Relevant Party's or RDP's completion of and exit from SREPT:

- all tests have been executed and results have been documented by the Relevant Party or RDP and evidence captured in the Relevant Party or RDP's Test Management Tool (or other system) and provided to the DCC;

- all testing issues identified during a Relevant Party's test execution have been recorded in the Test Management Tool. Of those Testing Issues either:
  - the Testing Issue generated by the Relevant Party as a result of its UEPT has been fixed and verified by retest; or
  - where outstanding, the Testing Issue has been reviewed and documented, and been included as part of a remediation plan that outlines the next steps to be taken, including estimated timescales required to resolve each of their outstanding Testing Issues. The remediation plan must be agreed by the DCC;
- any outstanding Testing Issue count must not exceed those defined in Table 6 - Testing Issue Threshold below:

Severity***	Threshold for Outstanding Testing Issues
1	0
2	0
3	5*
4	10*
5	As agreed**

Table 6 Testing Issue Threshold

* - Work around and remediation plan to be agreed with the DCC for each issue that ensures no impact on other Users

** - As agreed with the DCC, requiring no impact on market operations

*** - Refer to Appendix G for definitions of Issue severities.

- A Test Completion Report has been created by the Relevant Party or RDP and approved by the DCC; and
- A Quality Gate Review meeting has been held between the Relevant Party or RDP and the DCC, with progress approved by the DCC.

Pursuant to Section H14.25, where the DCC considers that a Relevant Party or RDP has not met the SREPT Exit Criteria, the Relevant Party or RDP may refer the matter to the Panel.

Where a dispute regarding whether a Relevant Party or RDP has met the SREPT Exit Criteria occurs, the SREPT Completion process will not resume whilst the dispute is being heard by the Panel, or until the SREPT Exit Criteria are met by the Relevant Party or RDP.

5.5.3 Quality Gate Review

Evidence of test completion may be requested for all or any of the tests during the Quality Gate Review, and irrespective of whether the information is reviewed, it shall be retained by the Relevant Party or RDP and may be requested by DCC at a later date.

Any remediation plan shall be discussed by the DCC and the Relevant Party or RDP and agreed as part of the evidence review.

A final decision regarding whether a Relevant Party or RDP has successfully completed SREPT will be provided to the Relevant Party or RDP no later than 2 Working Days after the date on which the Quality Gate Review meeting is held.

In addition, pursuant to Section H14.28, the DCC shall confirm on request by the Relevant Party or RDP whether or not it considers that the Relevant Party or RDP has successfully completed SREPT.

5.5.4 SREPT Test Completion Certificate

The Test Completion Certificate shall be issued by the DCC to the Relevant Party or RDP once the Quality Gate Review has concluded that the Relevant Party or RDP has met the SREPT Exit Criteria.

5.6. SREPT Regression Testing

DCC shall inform all Relevant Parties and RDPs undertaking SREPT and all Relevant Parties and RDPs that have completed SREPT of any change to DCC Systems that may affect SREPT.

Where the DCC deems that a change to DCC Systems necessitates Regression Testing, DCC may require Relevant Parties and RDPs to perform Regression Testing of the SREPT.

Where DCC does not require Relevant Parties or RDPs to perform Regression Testing, the decision as to whether Regression Testing is performed as a consequence of a change to DCC Systems or a change to User Systems, rests with the Relevant Party or RDP.

Where a Relevant Party or RDP performing Regression Testing has already completed SREPT, the Test Completion Certificate shall remain effective.

6. Appendix A: Test Artefacts

The DCC and each Relevant Party or RDP will be required to produce and maintain a number of documents, dashboards and reports during the testing lifecycle as depicted in Figure 1 Test Documentation Hierarchy, below.

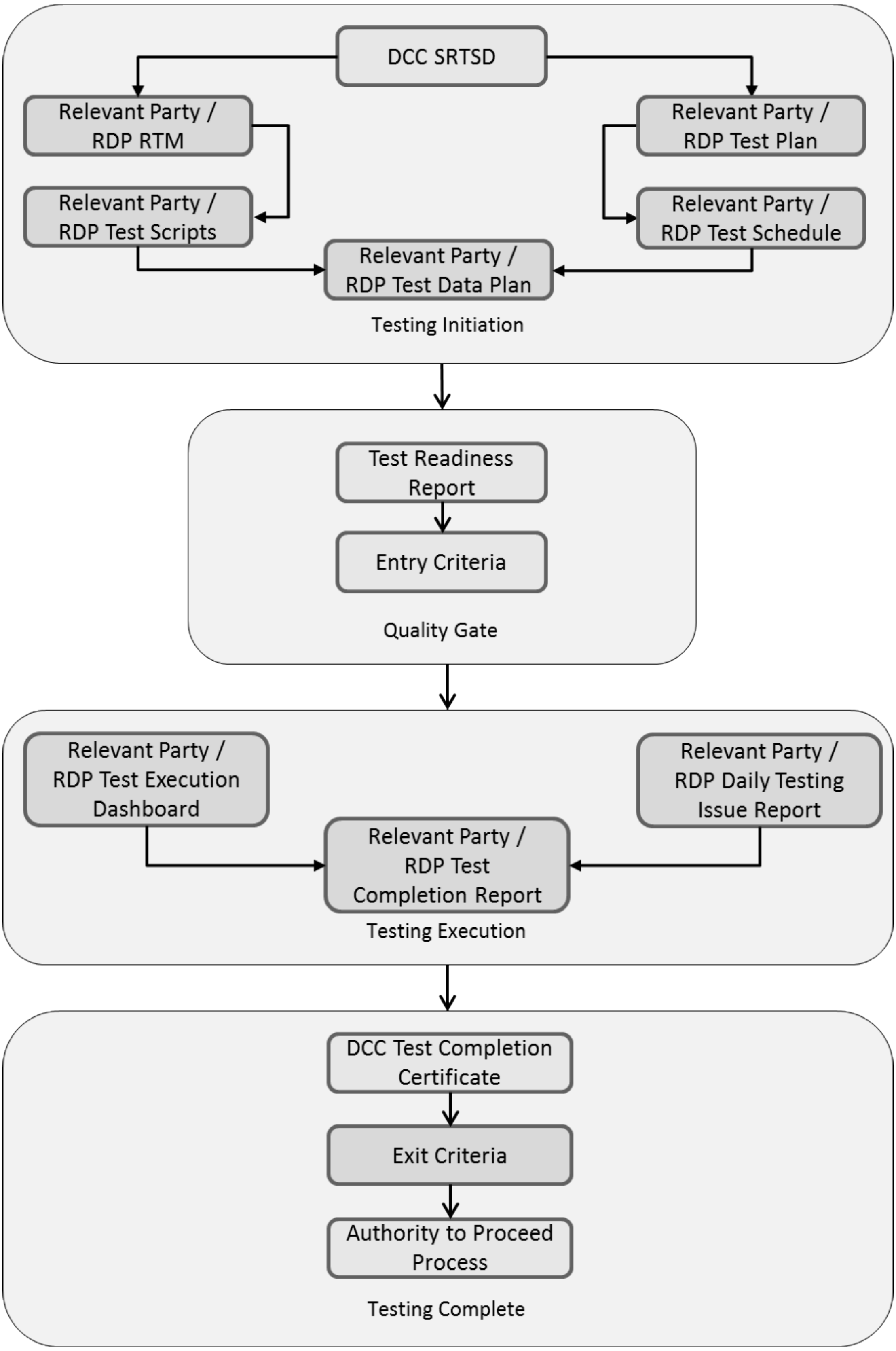

DCC SRTSD
Relevant Party / RDP RTM
Relevant Party / RDP Test Plan
Relevant Party / RDP Test Scripts
Relevant Party / RDP Test Schedule
Relevant Party / RDP Test Data Plan
Testing Initiation
Test Readiness Report
Entry Criteria
Quality Gate
Relevant Party / RDP Test Execution Dashboard
Relevant Party / RDP Daily Testing Issue Report
Relevant Party / RDP Test Completion Report
Testing Execution
DCC Test Completion Certificate
Exit Criteria
Authority to Proceed Process
Testing Complete

Figure 1 Test Documentation Hierarchy

6.1. Relevant Party or RDP Documents & Reports

6.1.1 Test Preparation Document Set

The following documentation must be produced by a Relevant Party or RDP before Testing commences:

- Test Readiness Report
- Scope of SREPT testing
- Test Plan
- Test Data Plan
- Test Schedule
- Requirements Traceability Matrix
- Test Scripts

Note regarding scope of SREPT testing - which SREPT test scenarios need to be undertaken is determined by:

- which SMKI interface or SMKI Repository Interface the Relevant Party or RDP will access and whether this is for Device Certificates or Organisation Certificates; and
- whether access to the SMKI interfaces will be through a DCC Gateway Connection or using the SMKI Portal interface via the Internet.

6.1.2 Reports and Dashboard

Table 7 Test Stage Supporting Documentation Set sets out the Reports and Dashboard that a Relevant Party or RDP must produce to demonstrate progress in preparing for and executing testing.

6.1.3 Test Readiness Report (TRR)

The Test Readiness Report shall be produced by the Relevant Party or RDP.

The report must be provided to the DCC by the Party or RDP on a weekly basis, commencing 40 Working Days prior to the start of Testing and must indicate progress against the following criteria:

- Previous Test Phase / Stage Exit Criteria (if appropriate);
- Relevant Party or RDP Test Management tool selected and available;
- Relevant Party or RDP key RAID (Risk, Assumption, Issue and Dependency) items, including, for each key item that has the potential to cause significant disruption to the commencement and / or completion of SMKI & Repository Entry Process Testing:
    - Priority (High, Medium, Low);
    - Severities of open issues;

    - Action taken;
    - Target close date; and
    - Overall RAG status (based on progress to plan);
- Relevant Party or RDP Test Plan produced;
- Relevant Party or RDP Test Schedule produced;
- Relevant Party or RDP Requirements Traceability Matrix containing:
    - Total numbers of Requirements identified;
    - Total number of testable requirements documented;
    - Total number of testable requirements in progress;
    - Total number of testable requirements not started; and
    - Total number of Requirements deemed not testable; and
- Relevant Party or RDP Test Script complete to date – to reflect the following breakdown:
    - Planned number of Test Scripts;
    - Total number of Test Scripts produced to date;
    - Total number of Test Scripts in progress;
    - Total number of Test Scripts not started;
    - % Test Data readiness by Party against planned Test Scripts;
    - Readiness of Party or RDP Test Resources and Technical (support) Resource;
    - Relevant Party or RDP test environment readiness – to include;
        - Security code of connection satisfied;
        - All interfaces required to support testing; and
    - Overall RAG status (based on likelihood of starting to plan).

6.1.4 Test Execution Dashboard

The Test Execution Dashboard will identify the Relevant Party or RDP's progress when executing testing and will be provided in a format specified by the DCC. The dashboard must be updated by the Relevant Party or RDP and provided to the DCC on a daily basis once testing commences, or per an alternative schedule agreed with the DCC.

The dashboard will include the following details:

- Name of Relevant Party or RDP, Party or RDP IDs under test;
- Location of Relevant Party or RDP testing;
- Date and time test execution dashboard updated by Relevant Party or RDP;
- Total number of tests Relevant Party or RDP scheduled for execution and projected as a test execution glide path;
- Actual number of tests executed by Relevant Party or RDP to date reflected on an incremental daily count including test results (passed, failed, blocked, not run, Ready for Test);
- Relevant Party or RDP summary of Testing Issues to include:
    - Total number of Testing Issues generated
    - Counts by status Open, Fixed, Closed etc.
    - Counts by Severity 1, 2, 3 etc.
    - Counts by Priority
    - Escalated to Issue Resolution Board (IRB).
- Relevant Party or RDP Regression Test execution results;
- Relevant Party or RDP summary progress against Exit Criteria;
- Relevant Party or RDP top 5 risks and issues – to include any environment concerns; and
- Relevant Party or RDP overall RAG status (based on progress against testing schedule).

6.1.5 Test Completion Report

The Relevant Party or RDP shall produce a Test Completion Report and submit the draft to the DCC 10 working days prior to the test completion date or at such time as agreed between DCC and the Party or RDP. The finalised version of the Test Completion Report will be submitted to the DCC on completion of each test execution activity.

A Test Completion Report template will be provided by the DCC to ensure that all Relevant Party or RDP reports contain the same level of detail. The report will include:

- Relevant Party or RDP Test approach and Scope of Testing Undertaken;
- Details of updates made to the test environment during the course of testing;
- Relevant Party or RDP Summary of the Test Results;
- Total number of tests originally scheduled for execution;
- Total number of tests executed;

- A table of tests run to include:
  - Overall results achieved ('Passed', 'Failed', 'Blocked', 'Not Run'); and
  - Any tests not run, blocked or not successfully executed end to end must be supported by an explanation.
- Relevant Party or RDP Summary of Testing Issues:
  - Total number of Testing Issues generated;
  - Total counts by status Open, Fixed, Closed; and
  - Total counts by Severity.

6.1.6 Test Traceability

To provide the DCC with a sufficient level of test assurance, all tests executed by each Relevant Party or RDP undertaking SREPT will be required to demonstrate full traceability as follows:

- Each requirement captured in the Requirements Traceability Matrix that can be tested during SREPT must be linked to one or many Test Scripts;
- Each Test Script executed must be reflected in one or many test execution cycles;
- A record of each test executed and the results of that test;
- Where an executed test generates a Testing Issue;
  - each Testing Issue must be linked to the test that generated the Testing Issue;
  - any subsequent retesting to validate a fix of Testing Issue carried out must be linked to the Testing Issue; and
  - each retest executed must reflect a result achieved as a result of execution.

6.1.7 Test Scripts

A Relevant Party or RDP shall develop its own test scripts and demonstrate how those test scripts meet the requirements in accordance with H14.26.

Test Stage Supporting Documentation Set

No	Phase	Description	DCC Responsibility	Relevant Party or RDP Responsibility	When/Frequency	Entry Criteria	Exit Criteria	Sign-Off Authority

1	Initiation	Guide to the SMKI and Repository Entry Process Tests	Produce and maintain	None	Prior to commencement of SREPT	N	N	DCC
2	Initiation	Test Data Plan (Device CSRs)	Produce	Use, if required	Prior to commencement of SREPT	N	N	DCC
3	Initiation	Test Plan including Test Schedule	Review and Approve	Produce and maintain	Test Stage Entry Quality Gate and updated during execution as required in preparation for Test Stage Exit Quality Gate	Y	Y	DCC
4	Initiation	Requirements Traceability Matrix	Review and Approve	Produce and maintain	Test Stage Entry Quality Gate and updated during execution as required in preparation for Test Stage Exit Quality Gate	Y	Y	DCC
5	Initiation	Test Scripts	Review and Approve	Produce and maintain	Test Stage Entry Quality Gate and updated during execution as required in preparation for Test Stage Exit Quality Gate	Y	Y	DCC
6	Initiation	Test Data Plan	Review	Produce and maintain	Test Stage Entry Quality Gate and updated during execution as required in preparation for Test Stage Exit Quality Gate	Y	N	DCC
7	Initiation	Test Readiness Review Checklist	Provide Template Review and Approve	Produce and maintain	Test Stage Entry Quality Gate	Y	N	DCC
8	Initiation	Test Stage Entry Criteria (part of final Test Readiness Report)	Review and Approve	Produce	Test Stage Entry Quality Gate	Y	N	DCC

9	Execution	Test Execution Dashboard	Review	Produce and maintain	Produced and updated daily (or other schedule agreed with the DCC) during execution in preparation for Test Stage Exit Quality Gate	N	Y	DCC
10	Execution	Testing Issue Report (part of the Test Execution Dashboard)	Review	Produce and maintain	Produced and updated daily (or other schedule agreed with the DCC) during execution in preparation for Test Stage Exit Quality Gate	N	Y	DCC
11	Execution	Test Completion Report	Provide Template Review and Approve	Produce and file	Test Stage during execution in preparation for Test Stage Exit Quality Gate	N	Y	DCC
12	Execution	Test Stage Quality Gate Exit Criteria (part of Test Completion Report)	Review and Approve	Produce	Test Stage Exit Quality Gate	N	Y	DCC

Table 7 Test Stage Supporting Documentation Set

Once these steps are complete the DCC will issue a Test Completion Certificate (see section 10).

7. Appendix B: Test Data

A Test Data Plan will be developed by the Relevant Party and coordinated with DCC in accordance with Section 5.4.1.3. The DCC and Relevant Party will be responsible for set up of Test Data on their respective system which must be defined in the Relevant Party Test Data Plan. The Data defined will be based on the following principles;

- No personal data which identifies any individual will be used for testing, but anonymised live Data is acceptable;
- Test Data will be representative of data likely to be used in the live environment once the Relevant Party is eligible in the relevant User Role; and
- A full range of Test Data covering all services to be tested will be used.

The DCC shall ensure that data supplied by the DCC for the purposes of testing is segregated when testing is being conducted by multiple Relevant Parties.

Table 8 Test Data Responsibilities below outlines the responsibilities in regard to preparing Test Data required to support UEPT.

Deliverable / Activity	Accountable / Responsible	Support
Test Data Preparation	DCC Licensee, Relevant Party or RDP	DSP

Table 8 Test Data Responsibilities

The DCC shall not provide the Relevant Party or RDP with Certificate Signing Requests (CSRs) in respect of either IKI Certificates or Organisation Certificates. Instead, a Relevant Party or RDP shall provide sufficient test data to be able to demonstrate its capability to produce CSRs for test Organisation Certificates in accordance with ETAD. The DCC shall provide Device CSRs for those Parties who are not able to provide their own to be able to undertake Device-related SMKI interface testing.

8. Appendix C: Test Scenarios

8.1. SMKI & Repository Entry Process Test Scenarios with DCC Gateway Connection

The following sub sections contain the SMKI & Repository Entry Process Test Scenarios that are applicable to each prospective user of SMKI & Repository Services that have access to a DCC Gateway Connection.

8.1.1 Security Credentials Access Tests for Test SMKI Service

ID	SMKI 02
Title:	Access the test SMKI Service, through the SMKI Portal interface over the DCC Gateway Connection.
Description	A Party / RDP's SMKI Authorised Responsible Officer (SMKI ARO) accesses the Test SMKI Services, through the SMKI Portal interface via the DCC Gateway Connection, using the security credentials supplied by the DCC.
Objective	• To prove that the SafeNet[1] Client Installed on the SMKI ARO's computer validates their security credentials. • To prove that a Party / RDP's ARO can use the FIPS Token which is registered to them and their organisation when accessing the SMKI Portal interface via the DCC Gateway Connection for Organisation Certificates and / or Device Certificates (as required).

ID	SMKI 03
Title:	Access the Test SMKI Services, through the Ad Hoc Device CSR Web Service interface and the Batched Device CSR Web Service interface, over a DCC Gateway Connection.

[1] The DCC makes available to PKI Client software (SafeNet Client), as set out in section 2.3.1 of the SMKI Code of Connection.

Description	A Party's system using the IKI security credentials supplied by the DCC accesses the Test SMKI Services, through the Ad Hoc Device CSR Web Service interface and the Batched Device CSR Web Service interface over a DCC Gateway Connection.

Objective	• To prove that the Party can access the Test SMKI Services through the Ad Hoc Device CSR Web Service interface and Batched Device CSR Web Service interface, as required, using the relevant IKI credentials. • To prove IKI credentials correctly authenticate to the SMKI web service interfaces.

8.1.2 Security Credentials Access Tests to the test SMKI Repository

ID	SMKI 05
Title:	Access the test SMKI Repository through the SMKI Repository Portal interface over a DCC Gateway Connection.
Description	A Party / RDP's SMKI ARO uses their individual IKI security credentials to access the test SMKI Repository through the SMKI Repository Portal interface.
Objective	• To prove access for the Party / RDP's ARO to the test SMKI Repository using the SMKI Repository Portal interface using the SMKI Repository URL, username and password.

ID	SMKI 06
Title:	Access the test SMKI Repository via the SMKI Repository Web Service interface over a DCC Gateway Connection.
Description	The Party's system uses the API Key issued by the DCC to access the test SMKI Repository using the SMKI Repository Web Service interface.
Objective	• To prove that the Party's system can access the test SMKI Repository using the SMKI Repository Web Service interface.

ID	SMKI 07
Title:	Access the test SMKI Repository through the SSH File Transfer Protocol (SFTP) interface over a DCC Gateway Connection.

Description	The Party / RDP's system or ARO uses the security credentials provided by the DCC to access the test SMKI Repository through the SMKI Repository SFTP (SSH File Transfer Protocol) interface.

Objective	• To prove that the Party / RDP's system or ARO can access the test SMKI Repository through the SMKI Repository SSH (Secure File Transfer Protocol) interface.

8.1.3 Submission of CSRs and Receipt of Certificates

ID	SMKI 22

Title:	Submit Organisation Certificate Signing Requests and receive the resulting Organisation Certificates through the SMKI Portal interface over a DCC Gateway Connection.

Description	A Party / RDP's SMKI Authorised Responsible Officer (SMKI ARO) submits an Organisation CSR and receives an Organisation Certificate for that CSR through the SMKI Portal interface.

Objective	• To prove a Party / RDP can generate and submit an Organisation CSR in the format specified in the SMKI Interface Design Specification. • To prove that a Party / RDP can download Organisation Certificates issued in respect of the submitted CSRs, and to confirm the information contained in the issued Organisation Certificate is consistent with the information contained within the corresponding CSR. • To prove that an Organisation Certificate can be rejected by the Party / RDP (according to the mechanism set out in the SMKI RAPP and / or specified in the SMKI Interface Design Specification).

ID	SMKI 23

Title:	Submit a Device Certificate Signing Request and receive a Device Certificate through the SMKI Portal interface over a DCC Gateway Connection.

Description	A Party's SMKI ARO submits a Device CSR and receives a Device Certificate for that Device CSR through the SMKI Portal interface.

Objective	• To prove that the Party's ARO can use the SMKI Portal Interface to submit a Device Certificate Signing Request.

	• To prove that the Party can use the SMKI Portal Interface to download individual Device Certificates and confirm the information contained in the issued Device Certificate is consistent with the information contained within the corresponding submitted Device CSR. • To prove that the issued Device Certificate can be rejected by the Party (according to the mechanism set out in the SMKI RAPP and / or specified in the Portal specification).

ID	SMKI 24

Title:	Submit Batched Certificate Signing Requests and receive Device Certificates through the SMKI Portal interface over a DCC Gateway Connection.

Description	A Party's SMKI ARO submits a Batched Certificate Signing Request and receives Device Certificates for each valid Device CSR through the SMKI Portal interface.

Objective	• To prove that the Party's SMKI ARO can use the SMKI Portal Interface to submit Batched Certificate Signing Request. • To prove that Device CSRs are batched correctly by the Party. • To prove that the Party can use the SMKI Portal Interface to download Device Certificates issued from the Batched Certificate Signing Request. • To prove that the issued Device Certificates are also lodged in the test SMKI Repository.

ID	SMKI 25

Title:	Submit a Device Certificate Signing Request and receive Device Certificate through the Ad Hoc Device Web Service interface over a DCC Gateway Connection.

Description	A Party's system submits a Device CSR and receives a Device Certificate through the Ad Hoc Device CSR Web Service interface.

Objective	• To prove that the Party's system can submit a Device CSR through the Ad Hoc Device Web Service interface. • To prove that the Party can receive a Device Certificate issued in respect of the submitted Device CSR from the Ad Hoc Device Web Service. • To prove that the issued Device Certificate is lodged in the test SMKI Repository.

ID	SMKI 57[2]
Title:	Submit Batched Certificate Signing Requests and receive Device Certificates through the Batched Device CSR Web Service interface over a DCC Gateway Connection.
Description	A Party's system submits Batched Certificate Signing Requests and receives Device Certificates through the Batched Device CSR Web Service interface.
Objective	• To prove that the Party's system can use the Batched Device CSR Web Service interface to submit Batched Certificate Signing Requests. • To prove that Device CSRs are batched correctly by the Party. • To prove that Parties can download their Device Certificates issued in respect of Batched Certificate Signing Requests. • To prove that the issued Device Certificates are also lodged in the test SMKI Repository.

8.1.4 Download Certificates from the test SMKI Repository

ID	SMKI 29
Title:	Download a copy of all 'In Use' SMKI Test Certificates from the test SMKI Repository through the SFTP (SSH File Transfer Protocol) interface over a DCC Gateway Connection.
Description	Using a file transfer client the Party downloads a copy of all in use SMKI Certificates from the test SMKI Repository via SFTP (SSH File Transfer Protocol) interface.
Objective	• To prove that the Party / RDP can use a file transfer client that supports SFTP in accordance with the standards in the SMKI Repository Interface Design Specification to access the SFTP interface. • To prove that the Party / RDP's file transfer client can download a complete copy of all in use Certificates (including OCA and DCA Certificates).

ID	SMKI 30

[2] Subject to delivery of the Change Request to deliver this functionality.

Title:	Download a daily delta file of SMKI Test Certificates through the SFTP interface over a DCC Gateway Connection.

Description	Using a file transfer client the Party / RDP downloads a partial / daily ‘delta file’ copy of all SMKI Certificates issued in the preceding twenty four hours from the test SMKI Repository via SFTP (SSH File Transfer Protocol) interface.

Objective	• To prove that the Party / RDP’s file transfer client can download a partial/’Daily Delta File’ batch containing Certificates published to the test SMKI Repository during the preceding twenty four hours (including OCA and DCA Certificates).

8.1.5 Query the test SMKI Repository and Retrieve Certificates

ID	SMKI 31

Title:	Query the test SMKI Repository for Organisation Certificates through the SMKI Repository Portal interface over a DCC Gateway Connection.

Description	A Party / RDP’s SMKI ARO uses the SMKI Repository Portal Interface to query the test SMKI Repository for an Organisation Certificate and downloads the Organisation Certificate.

Objective	• To prove the Party / RDP’s ARO is able to use the SMKI Repository Portal Interface. • To prove that the Party / RDP’s ARO can query the test SMKI Repository using the SMKI Repository Portal interface to locate an Organisation Certificate in the test SMKI Repository. • To prove a Party / RDP’s ARO is able to download the located Organisation Certificate.

ID	SMKI 32

Title:	Query the test SMKI Repository for Organisation Certificates through the SMKI Repository Web Service interface over a DCC Gateway Connection.

Description	A Party / RDP’s system queries the test SMKI Repository for an Organisation Certificate via the SMKI Repository Web Service interface and retrieves the Organisation Certificate.

Objective	• To prove the Party / RDP's system is able to use the SMKI Repository Web Service interface. • To prove that the Party / RDP's system can query the test SMKI Repository using the SMKI Repository Web Service interface to locate an Organisation Certificate in the test SMKI Repository. • To prove the Party / RDP's system can receive the located Organisation Certificate.

ID	SMKI 33

Title:	Query the test SMKI Repository for Device Certificates through the SMKI Repository Portal interface over a DCC Gateway Connection.

Description	A Party's SMKI ARO uses the SMKI Repository Portal interface to query the test SMKI Repository for a Device Certificate and downloads the Device Certificate.

Objective	• To prove the Party's ARO is able to use the SMKI Repository Portal Interface (if not already done as part of SMKI 31). • To prove that the Party's ARO can query the test SMKI Repository using the SMKI Repository Portal interface to locate a Device Certificate in the test SMKI Repository. • To prove a Party's ARO is able to download the located Device Certificate.

ID	SMKI 34

Title:	Query test SMKI Repository for Device Certificates through the SMKI Repository Web Service interface over a DCC Gateway Connection.

Description	A Party's system queries the test SMKI Repository for a Device Certificate via the SMKI Repository Web Service interface and retrieves a Device Certificate.

Objective	• To prove the Party's system is able to query the test SMKI Repository to determine the presence of a Device Certificate in the test SMKI Repository. • To prove a Party's system can retrieve the located Device Certificate.

8.1.6 Obtain Organisation Certificate Revocation List and Organisation Authority Revocation List

ID	SMKI 48
Title:	Obtain the Organisation Certificate Revocation List (CRL) and Organisation Authority Revocation List (ARL) through the SMKI Repository Portal interface over a DCC Gateway Connection.
Description	A Party / RDP's SMKI ARO wishes to access the Organisation CRL and ARL using the SMKI Repository Portal interface via a DCC Gateway Connection.
Objective	• To prove that a Party / RDP's SMKI ARO can access and / or download the Organisation CRL and Organisation ARL using the SMKI Repository Portal interface via DCC Gateway Connection.

ID	SMKI 50
Title:	Obtain the latest Organisation CRL and Organisation ARL through using the URL to the SMKI Repository over a DCC Gateway Connection.
Description	The Party / RDP's system accesses the test SMKI Repository using URL to obtain the latest Organisation CRL and Organisation ARL.
Objective	• To prove that a Party / RDP's system can access and / or download the latest Organisation CRL and Organisation ARL using the URL to the SMKI Repository.

8.2. SMKI & Repository Entry Process Test Scenarios without DCC Gateway Connection

The following sub sections contain the SMKI & Repository Entry Process Test Scenarios that are applicable to each prospective user of SMKI & Repository Services that do not have access to a DCC Gateway Connection.

8.2.1 Security Credentials Access Tests to SMKI

ID	SMKI 04
Title:	Access the Test SMKI Service, through the SMKI Portal interface over the internet.

Description	For a Party without a DCC Gateway Connection, a SMKI ARO accesses the Test SMKI Service, through the SMKI Portal interface using the security credentials supplied by the DCC.

Objective	• To prove that the SafeNet Client Installed on the SMKI ARO's computer validates their security credentials. • To prove that a Party's ARO can use the FIPS Token which is registered to them and their organisation when accessing the SMKI Portal interface via the internet.

8.2.2 Submission of Organisation CSRs and Receipt of Organisation Certificates

ID	SMKI 26

Title:	Submit Organisation Certificate Signing Requests and receive Organisation Certificates through the SMKI Portal interface over the internet.

Description	For a Party without a DCC Gateway Connection, a SMKI ARO submits an Organisation CSR and receives an Organisation Certificate for that CSR through the SMKI Portal interface over the internet.

Objective	• To prove a Party can generate and submit an Organisation CSR in the format specified in the SMKI Interface Design Specification. • To prove that a Party can download Organisation Certificates issued in respect of the submitted CSRs, and to confirm the information contained in the issued Organisation Certificate is consistent with the information contained within the corresponding CSR. • To prove that an Organisation Certificate can be rejected by the Party (according to the mechanism set out in the RAPP and / or specified in the Portal specification.

8.2.3 Submit requests for SMKI Repository content and obtain Certificates

ID	SMKI 08

Title:	Submit requests for and receive SMKI Repository content using the SMKI Portal interface over the Internet.

Description	For a Party without a DCC Gateway Connection, an SMKI ARO accesses the SMKI Portal interface and makes a request for and receives content from the test SMKI Repository.

Objective	• To prove that a Party's SMKI ARO can use the SMKI Portal interface to request and receive the latest Organisation CRL and latest Organisation ARL.

ID	SMKI 38
Title:	Download Organisation Certificates and OCA Certificates through the SMKI Portal interface over the internet.
Description	For a Party without a DCC Gateway Connection, a SMKI ARO accesses the SMKI Portal interface over the Internet, locates and downloads Organisation Certificates that are required to be installed on Devices ahead of installation.
Objective	• To prove that the Party's ARO can locate and download the zip file of Organisation Certificates through the SMKI Portal over the internet.

9. Appendix D: Forms and Templates

Extant versions of templates for the following documents will be maintained on the DCC Website or SharePoint. The following templates are provided in this document to support the consultation process:

Section	Template
9.1	Party / RDP Notification of Intention to Undertake Testing Template
9.2	DCC Acknowledgement of Intention to Undertake Testing Template
9.3	Test Readiness Report Template
9.4	Test Plan Template
9.5	Test Execution Dashboard Template
9.6	Test Completion Report Template

9.1. Party / RDP Notification of Intention to Undertake Testing Template

To:[DCC]

From:[PARTY / RDP]

Date: [Date]

Dear Sir or Madam,

PARTY / RDP NOTIFICATION OF INTENTION TO UNDERTAKE TESTING

TEST: SMKI and REPOSITORY ENTRY PROCESS TESTS

We hereby give notice that we intend to undertake SMKI and Repository Entry Process Tests in accordance with the SMKI & Repository Test Scenarios Document.

The required information is provided in the table below:

Party / RPD	SEC Party / RDP ID	Test Start Date	Name, Email & Phone Number of Test Manager

Yours faithfully

[Name]

[Position]

Acting on behalf of [Party].

9.2. DCC Acknowledgement of Intention to Undertake Testing Template

To:[PARTY / RDP]

From:[DCC]

Date:[Date]

Dear Sir or Madam,

DCC ACKNOWLEDGEMENT OF INTENTION TO UNDERTAKE TESTING

TEST: SMKI & REPOSITORY ENTRY PROCESS TESTS

We hereby acknowledge your notification that you intend to undertake SMKI & Repository Entry Process Tests in accordance with the SMKI & Repository Test Scenarios Document.

The table below confirms the contact details of our Test Manager and the date of the SMKI & Repository Entry Process Test (SREPT) Initiation Meeting:

Party / RDP	SEC Party / RDP ID	Test Start Date	Name, Email & Phone Number of DCC User Entry Process Test Manager	Date of SREPT Initiation Meeting

Yours faithfully

[Name]

[Position]

Acting on behalf of the DCC.

9.3. Test Readiness Report Template

To:[DCC]

From:[PARTY / RDP]

Date:[Date]

Dear Sir or Madam,

TEST READINESS REPORT

TEST: SMKI & REPOSITORY ENTRY PROCESS TESTS

We hereby provide our current assessment of our readiness to conduct SMKI & Repository Entry Process Tests for:

Overview:

Party / RDP: [Party / RDP]

Test Start Date: [Test Start Date]

Report Information:

Date of Report: [Date]

Period Covered by Report: [From date to date]

Produced by: [Name of Reporter]

Readiness Information:

Overall RAG: [Red / Amber / Green]

Test Tool Selected & Available: [Y / N]

Party Test Plan produced: [Y/N]

Party Test Schedule produced: [Y/N]

Risks, Assumptions, Issues & Dependencies (RAID):

Please detail key RAID (Risk, Assumption, Issue and Dependency) items that have the potential to cause significant disruption to the commencement and / or completion of SMKI & Repository Entry Process Testing

RAID Description	Priority(H/M/L)	Action Taken	Target Close Date	RAG Status (R/A/G)

Requirements Traceability Matrix Progress:

RTM Information Required	Response
Requirements Traceability Matrix complete to date (%)	
Numbers of Requirements identified (number)	
Number of testable requirements in progress (number)	
Number of testable requirements not started (number)	
Number of Requirements deemed not testable (number)	

Test Script Development Progress:

Test Script Information Required	Response
Test Scripts complete to date (%)	
Planned number of Test Scripts (number)	
Number of Test Scripts produced to date (number)	
Number of Test Scripts in progress (number)	
Number of Test Scripts not started (number)	

Test Data readiness by Party against planned Test Scripts (%)	

Resources & Environments Progress:

Resources & Environments Information Required	Response
Test Resources & Technical (support) Resource Ready (Y/N if N, date expected to be ready)	
Environment Readiness:	
All interfaces required to support testing (Y/N)	

Environments information:

[Environment configuration approved as suitable – to include breakdown and description of hardware]

SREPT Entry Criteria (to be completed by final report):

Entry Criteria	Complete (Y/N)
Confirm that the person requesting to commence testing is a SEC Party / RDP	
Party / RDP has identified the SMKI Interfaces the Party or RDP will access and whether this is for Device or Organisation Certificates and whether access will be through a DCC Gateway Connection	
Party has produced relevant test artefacts in sections 5.3.1.1, 5.3.1.5, and 5.3.1.6 of the SMKI & Repository Test Scenarios Document:	
- Party Notification of Intention to Undertake Testing	
- Test Readiness Report (this document)	
- Test Plan incorporating the Test Schedule	
- Requirements Traceability Matrix	

- Test Scripts	

- Test Data Plan	

has complied with the procedural steps for initiating SREPT (as set out in Table 2 of the SRTSD	

Party has provided evidence to the DCC that a test environment capable of supporting the planned testing has been established and is available	

Party has provided evidence to the DCC that an appropriate level of resources are available to support the SREPT process	
Party has provided confirmation that the Security Requirements set out in the Enduring Testing Approach Document have been met	

Overall Status:

Overall Status (R/A/G)
R – testing start in line with planned date is not achievable
A – testing start in line with planned date is at risk
G – testing is expected to start on the planned date

End of report.

Yours faithfully

[Name]

[Position]

Acting on behalf of [Party / RDP].

9.4. Test Plan Template

To: [DCC]

From: [PARTY / RDP]

Date: [Date]

Dear Sir or Madam,

TEST PLAN INCLUDING TEST SCHEDULE

TEST: SMKI & REPOSITORY ENTRY PROCESS TESTS

We hereby provide our Test Plan, in accordance with the SMKI & Repository Test Scenarios Document.

Overview:

Party: [Party / RDP]

Test Start Date: [Test Start Date]

Scope

[Textual description of testing scope].

Scenarios to be Tested

See the matrices in section 5 to determine the scenarios to be tested.

Reference to Section 5 (List all scenarios to be tested, as determined by the privileges requested, or to be requested, via the SMKI RAPP.

Approach

[Textual description of the following:

- *Test Scenarios & Scripts*
- *Test Cycles*

- *Re-Testing*
- *Regression*
- *Defect Management*
- *Test Data*
- *Tools]*

Test Schedule

[Provide a schedule of the testing that you will undertake. This can be the form of a Project Plan, or Spreadsheet, or other format agreed with the DCC.]

Resources

[Provide details of the resources required to support the testing set out above. This can be included in the Project Plan or Spreadsheet.

This should consider roles such as Test Manager, Test Lead, Senior Test Analysts, Test Analysts, IS Support Requirements.]

End of report.

Yours faithfully

[Name]

[Position]

Acting on behalf of [Party / RDP].

9.5. Test Execution Dashboard Template

To: [DCC]

From: [PARTY / RDP]

Date: [Date]

Dear Sir or Madam,

TEST EXECUTION DASHBOARD

TEST: SMKI & REPOSITORY ENTRY PROCESS TESTS

We hereby provide our Test Execution Dashboard, in accordance with the SMKI & Repository Test Scenarios Document.

Overview:

Party / RDP: [Party / RDP] Party /RDP ID: [Party / RDP ID]

Location: [Location of Testing / Test Manager]

Test Start Date: [Test Start Date]

Report Information:

Date & Time of Report: [Date, Time]

Period Covered by Report: [Date (for daily reports) or from date to date (for other reporting frequency]

Produced by: [Name of Reporter]

Progress Information:

[Please provide a 'Glide Path' for the testing you are undertaking, showing progress toward execution of 100% of the tests planned. This can be in the form of a spreadsheet or other format agreed with the DCC.]

Test Script Information Required	Number
Total Planned number of Tests (Test Readiness Report)	
Number of Tests scheduled for execution by report date	
Number of Tests executed by report date	

Number of Test passed by report date	
Number of Test failed by report date	
Number of Test blocked by report date	
Number of Test not run by report date	

Test Issue Report Information:

Testing Issue Information Required	Number
Number of Testing Issues generated	
Number of Testing Issues closed	
Number of Testing Issues open	
Number of open Testing Issues, by severity:	
- Severity 1	
- Severity 2	
- Severity 3	
- Severity 4	
- Severity 5	

Progress Toward Exit Information:

[Textual description of progress made so far toward completion of testing]

Progress Toward Exit Required	Date
Anticipated Completion Date (Submission of Test Completion Report)	

Risk Information:

Risk	Description	Target Close Date	RAG Status (R/A/G)

1			
2			
3			
4			
5			

Overall Status:

Overall Status (R/A/G)
R – testing start in line with planned date is not achievable
A – testing start in line with planned date is at risk
G – testing is expected to start on the planned date

9.6. Test Completion Report Template

To: [DCC]

From: [PARTY / RDP]

Date: [Date]

Dear Sir or Madam,

TEST COMPLETION REPORT

TEST: SMKI & REPOSITORY ENTRY PROCESS TESTS

We hereby provide our Test Completion Report, in accordance with the SMKI & Repository Test Scenarios Document.

Overview:

Party / RDP: [Party / RDP]

Test Start Date: [Test Start Date]

Approach and Scope of Testing Undertaken:

[Per the Test Plan, noting any variations.]

Summary of Test Results:

Test Script Information Required	Number
Number of tests originally scheduled for execution	
Number of tests originally scheduled for execution	
Number of tests passed	
Number of tests failed	
Number of tests not run	
Number of tests blocked	

Detail of Tests Not Successfully Executed:

Test	Explanation

Summary of Testing Issues:

Testing Issue Information Required	Number
Number of Testing Issues generated	
Number of Testing Issues closed	
Number of Testing Issues open	
Number of open Testing Issues, by severity:	
- Severity 1	
- Severity 2	
- Severity 3	
- Severity 4	
- Severity 5	

SREPT Exit Criteria Checklist:

Entry Criteria	Complete (Y/N)
Test Results have been documented by the Party and evidence captured in the Party's Test Management Tool and are available to be provided to the DCC	
Testing issues identified during a Party's test execution have been recorded in the Test Management Tool (see note, below)	
Test Completion Report has been created by the Party and approved by the DCC	

Note: All testing issues must either:

- been fixed and verified by retest; or
- where outstanding, have been reviewed and documented, and been included as part of a remediation plan that outlines the next steps to be taken, including estimated timescales required to resolve each of their outstanding Testing Issues. The remediation plan must be agreed by the DCC

End of report.

Yours faithfully

[Name]

[Position]

Acting on behalf of [Party].

10. Appendix E: Test Completion Certificate

TEST COMPLETION CERTIFICATE

To: [Party / RDP] [SEC Party / RDP ID]

From: [DCC]

[Date]

Dear Sirs,

TEST COMPLETION CERTIFICATE

The relevant tests have been successfully completed to provide the following credentials:

Test Scenarios for Parties or RDPs with a DCC Gateway Connection
IKI credentials for submission of Organisation CSRs using SMKI Portal via DCC Gateway Connection
IKI credentials for submission of Device CSRs using SMKI Portal via DCC Gateway Connection
IKI credentials for Ad Hoc Device CSR Web Service
IKI credentials for Batched Device CSR Web Service
Credentials for SMKI Repository Portal
Credentials for SMKI Repository Web Service
Credentials for SMKI Repository Portal SFTP

Test Scenarios for Parties without a DCC Gateway Connection
IKI credentials for submission of Organisation CSRs using SMKI Portal via the Internet

We confirm that the relevant tests have been executed in accordance with the relevant Test Documents. We confirm that the relevant Exit Criteria have been achieved.

Yours faithfully

[Name]

[Position]

Acting on behalf of the DCC

11. Appendix F: Definitions

In this document, except where the context otherwise requires:

- expressions defined in Section A of the Code (Definitions and Interpretation) have the same meaning as is set out in that Section;
- the expressions in the left hand column below shall have the meanings given to them in the right hand column below; and
- where any expression is defined in Section A of the Code (Definitions and Interpretation) and in this document, the definition in this document shall take precedence for the purposes of this document.

Term	Definition
Ad Hoc Device CSR Web Service	Has the meaning given to that expression in the SMKI RAPP
Batched Device CSR Web Service	Has the meaning given to that expression in the SMKI RAPP
Daily Testing Issue Report	The document reporting on the status of any testing issues identified (part of the Test Execution Dashboard)
Device Certificate Signing Request (Device CSR)	Means a Certificate Signing Request in respect of a Device Certificate.
FIPS token	Cryptographic Credential Token issued in accordance with the SMKI RAPP
Organisation Certificate Signing Request (Organisation CSR)	Means a Certificate Signing Request in respect of an Organisation Certificate.
Regression Testing	Testing of a previously tested program following modification to ensure that defects have not been introduced or uncovered in unchanged areas of the software, as a result of the changes made (and Regression Test shall be construed accordingly)
Relevant Party	A Party which is undertaking SMKI and Repository Entry Process Tests
(Requirements) Traceability Matrix	A matrix of defined requirements that provides traceability (linkage) to Test Scripts for the purpose of providing a measurement of test coverage as intended in the relevant specification.
SMKI Authorised Responsible Officer (SMKI ARO)	Has the meaning given to the expression 'Authorised Responsible Officer' in the SMKI RAPP.

SMKI Senior Responsible Officer (SMKI SRO)	Has the meaning given to the expression 'Senior Responsible Officer' in the SMKI RAPP.
SMKI Repository Portal	Has the meaning given to that expression in the SMKI Repository Interface Design Specification.
SMKI Repository Web Service	Has the meaning given to that expression in the SMKI Repository Interface Design Specification.
SREPT	SMKI and Repository Entry Process Tests
SREPTS	SMKI and Repository Entry Process Test Scenarios
SRTSD	SMKI and Repository Test Scenarios Document (this document)
Test Completion Certificate	A certificate issued by the on successfully completes SREPT as set out in Appendix E: Test Completion Certificate
Test Completion Report	A document summarising testing activities and results. It also contains an evaluation of the corresponding test items against Exit Criteria
Test Completion Certificate	A certificate issued by the DCC to the Party when the Party has met the SREPT Exit Criteria
Test Data	Any data constructed for the purposes of undertaking SMKI and Repository Entry Process Testing
Test Data Plan	The document that sets out: the size and type/format of data, who is responsible for providing the data; and when the data is required to be available to support test activities in a Test Plan
Test Execution Dashboard	The document summarising testing activities and results, produced at regular intervals, to report progress of testing activities against a baseline (such as the original test plan) and to communicate risks and alternatives requiring a decision to management
Test Management Tool	A tool that has the ability to log and track Testing Issues
Test Plan	A document describing the scope, approach, resources and schedule of intended test activities within a Test Stage that will be produced as set out in Section 9.4.
Test Result	The consequence/outcome of the execution of a Test Script
Test Readiness Report	A report that when completed provides the capability to assess the status of test preparation and determine the readiness to proceed into test execution
Test Schedule	A list of test process activities, tasks or events identifying their intended start and finish dates and/or times and interdependencies
Test Script	A document specifying a sequence of actions for the execution of a test

Test SMKI Repository Services	Test versions of the SMKI Repository Services (see definition in SEC) provisioned for the purposes of SREPT
Test SMKI Services	Test versions of the SMKI Services (see definition in SEC) provisioned for the purposes of SREPT
Test Stage	A group of test activities that are organised and managed together
WD	Has the same meaning as the expression 'Working Day'.

12. Appendix G: Testing Issue Severity Descriptions

Severity	Description
Severity 1	An Issue which in relation to the Relevant Party or RDP: • would prevent user from using their systems • would have a critical adverse impact on business activities • would cause significant financial loss • would result in any material loss or corruption of Data. Non-exhaustive examples: • an Issue leading to non-availability of systems • all test progress is blocked.
Severity 2	An Issue which in relation to the Relevant Party or RDP: • would have a major (but not critical) adverse impact on use of systems • would cause limited financial loss Non-exhaustive examples: • an Issue leading to non-availability of or to loss of resilience of a material part of their systems • large areas of functionality will not be able to be tested • testing not completely blocked but has been significantly impacted.
Severity 3	An Issue which in relation to the Relevant Party or RDP: • would have a major adverse impact on business activities but which can be reduced to a moderate adverse impact through a work-around • would have a moderate adverse impact on the business activities Non-exhaustive examples: • testing can progress but the work-around will impact test progress.
Severity 4	An Issue which in relation to the Relevant Party or RDP: • would have a minor adverse impact on business activities Non-exhaustive examples: • minor service interruptions in the business process
Severity 5	An Issue which in relation to the Relevant Party or RDP: • would have minimal impact on business activities Non-exhaustive examples: • trivial Issues with work-arounds which are noted for future releases but minimal impact of running existing activities • tests can still pass but there are cosmetic issues.

Version: L7.0

Appendix L

SMKI Recovery Procedure

1. Introduction

1.1 Purpose & Interpretation

Section L10.4 of the Code sets out the principal rights and obligations for compliance with any requirements set out in the SMKI Recovery Procedure.

This document, the SMKI Recovery Procedure, sets out the procedural requirements and the rights and obligations in respect of the DCC, Parties and the SMKI PMA relating to recovery from the Compromise of a Relevant Private Key. The scope of the SMKI Recovery Procedure is as set out in Section L10 of the Code and is further set out in more detail in Section 1.2 of this document.

The procedures as set out in this document shall be executed in the event of a Compromise of a Relevant Private Key, other than as directed by the SMKI PMA, in accordance with the procedures set out in this document.

For the purposes of the SMKI Recovery Procedure defined terms shall have the meaning in SEC Section A (Definitions and Interpretations), SEC Appendix B (Organisation Certificate Policy), and Appendix F (Definitions) of this SEC Appendix L (SMKI Recovery Procedure). Additionally, the following shall apply:

a) notwithstanding the definition as set out in Section A of the Code, “Subscriber” means, in relation to any Organisation Certificate associated with a Relevant Private Key, a Party which has been Issued with and accepted that Organisation Certificate, acting in its capacity as the holder of the Organisation Certificate;

b) “M#N Share” means, in relation to a Private Key, that the key is split into N Key Components such that the Private Key may be recreated using any M or more Key Components, and the Private Key may not be recreated using fewer than M Key Components;

c) except where explicitly stated otherwise, or where it would be inappropriate within the context of its use, the term "Compromise" shall be interpreted to be a reference to a Compromise or a suspected Compromise.

d) “Contingency Symmetric Key” means, as defined in the SEC Section A, the Symmetric Key used to encrypt the Contingency Public Key;

e) Relevant Private Key has, as defined in the SEC Section A, the meaning set out in Section L10;

f) "Recovery Action Risks" has the meaning defined in section 3.5 of this document;

g) "Party" has the meaning set out in SEC Section A except for the DCC, which shall not be a Party for the purposes of this document;

h) "TADP" means the Threshold Anomaly Detection Procedures;

i) "XML Signing Private Key" means a Private Key for which an associated Organisation Certificate has been issued that would allow the Subscriber to sign XML documents pursuant to the SEC. For clarity, this includes private keys which are (1) used by the DSP, or by a provider of WAN services to the DCC, only to sign XML and (2) have a GBCS defined Remote Party Role.

j) where an obligation is expressed as being an obligation on a Key Custodian it shall be interpreted as being an obligation on:

i. in the case of a Key Custodian appointed by a Party or the DCC, that Party or the DCC as the context requires, and

ii. in the case of a Key Custodian appointed by the SMKI PMA or the Panel, the SMKI PMA or the Panel Member as the context requires;

k) except for a Root OCA Certificate, a Private Key is “associated” with an Organisation Certificate or OCA Certificate where that Private Key is associated with the Public Key contained within that Organisation Certificate or OCA Certificate. For a Root OCA Certificate, a Private Key is "associated" with that Root OCA Certificate if it is associated with the Public Key contained in unencrypted form within that Root OCA Certificate. Note that a Contingency Public Key will also be present in a Root OCA Certificate but that it will be presented in an encrypted form;

l) "CoS Certificate" means an Organisation Certificate issued to the DCC, acting in the role of the CoS Party, which has a Remote Party Role of 'transitionalCoS' with the meaning of SEC Section L, clause 3.18;

m) an Organisation Certificate or OCA Certificate is considered to be “stored” on a Device if information from that Organisation Certificate or OCA Certificate forms part of the Device Security Credentials of that Device; and

n) “Contingency Symmetric Key Splitting” means the splitting of the Contingency Symmetric Key into parts, each of which are securely retained by each of the “Symmetric Key Custodians”. “Symmetric Key Custodians” shall be interpreted accordingly with the roles being fulfilled by the DCC.

1.2 Scope

The SMKI Recovery Procedure sets out the detail of the arrangements between the DCC, Parties, the SMKI PMA and the Panel in respect of:

a) **Pre-Recovery:**

i. confirmation of a Compromise of a Relevant Private Key that the DCC becomes aware of, including where this is reported to the DCC by a Party, resulting in an Incident being raised in accordance with sections 2.1 and 2.2 of the Incident Management Policy;

ii. notification to the DCC of the Anomaly Detection Thresholds (or amendment of Anomaly Detection Thresholds by the DCC where necessary, including where the DCC will be originating Commands as part of the recovery procedure) that are required to support replacement of affected Organisation Certificates or OCA Certificates stored on Devices;

iii. where use of the Recovery Private Key or the Contingency Private Key would be required in order to recover, consultation by the DCC with the SMKI PMA to determine the extent to which the recovery procedure should be executed and the manner in which it should be executed;

iv. revocation of affected Organisation Certificates or OCA Certificates (where required); and

v. other steps as set out in this SMKI Recovery Procedure;

b) **Execution of Recovery:**

i. execution of activities to recover from a Compromise of a Relevant Private Key; and

c) **Post-Recovery:**

i. replacement of Organisation Certificates and OCA Certificates and Private Keys (where necessary);

ii. post-Incident review and reporting;

iii. provision to relevant parties of information intended to prevent reoccurrence of similar Incidents; and

iv. revocation of replaced Organisation Certificates and OCA Certificates (where necessary).

The SMKI Recovery Procedure addresses recovery from a Compromise in respect of any Relevant Private Key listed immediately below:

a) Pursuant to L10.30 (c) (ii) and (iii):

i. a Private Key which is associated with any Organisation Certificate, Data from which is used to populate the Device Security Credentials of a Device comprising part of an Enrolled Smart Metering System; or

ii. a Private Key which is associated with any Organisation Certificate, Data from which is used to populate part of any Device Security Credentials held by an S1SP;

b) Pursuant to L10.30 (c) (i), the Contingency Symmetric Key;

c) Pursuant to L10.30 (c) (ii), the Contingency Private Key;

d) Pursuant to L10.30 (c) (iv), the Private Key associated with an Issuing OCA Certificate;

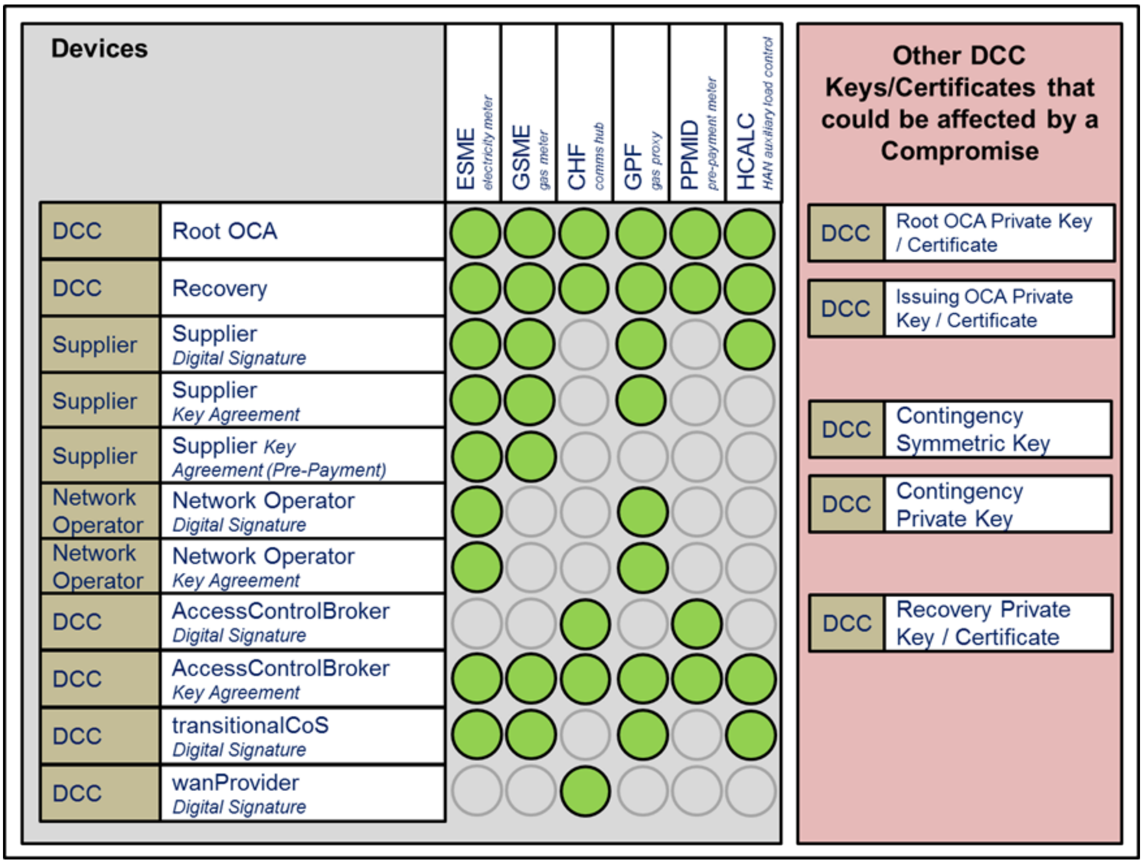
e) Pursuant to L10.30 (c) (ii) and (iv), the Private Key associated with a Root OCA Certificate;

f) Pursuant to L10.30 (c) (ii) the Private Key associated with a Recovery Certificate; and

g) Pursuant to L10.30 (c) (v), an XML Signing Private Key.

Pursuant to L10.30 (c) (vi, the relevant Certification Practice Statement (CPS) addresses recovery from a Compromise in respect of any Private Key which is associated with a Public Key contained in any certificate issued in accordance with an S1SPKI Certificate Policy, and which is determined by the SMKI PMA as being a Private Key requiring a recovery procedure.

Figure 1, immediately below, shows the relevant Organisation Certificates and OCA Certificates that are stored on applicable SMETS2+ Devices. The details listed in the column labelled 'ESME' apply both to Devices which are ESME and to Devices which are SAPC.

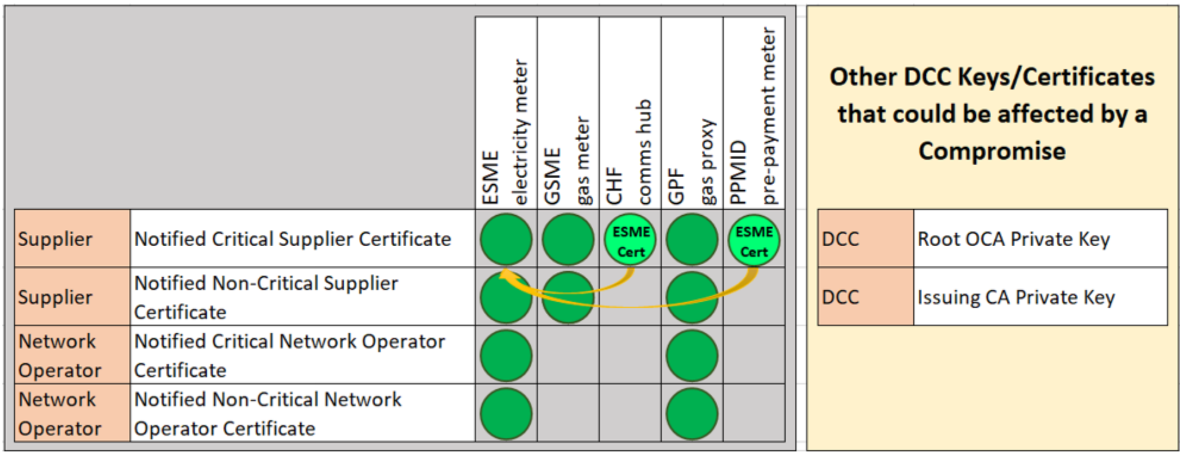


Devices		ESME *electricity meter*	GSME *gas meter*	CHF *comms hub*	GPF *gas proxy*	PPMID *pre-payment meter*	HCALC *HAN auxiliary load control*
DCC	Root OCA	●	●	●	●	●	●
DCC	Recovery	●	●	●	●	●	●
Supplier	Supplier *Digital Signature*	●	●	○	●	○	●
Supplier	Supplier *Key Agreement*	●	●	○	●	○	○
Supplier	Supplier *Key Agreement (Pre-Payment)*	●	●	○	○	○	○
Network Operator	Network Operator *Digital Signature*	●	○	○	●	○	○
Network Operator	Network Operator *Key Agreement*	●	○	○	●	○	○
DCC	AccessControlBroker *Digital Signature*	○	○	●	○	●	○
DCC	AccessControlBroker *Key Agreement*	●	●	●	●	●	●
DCC	transitionalCoS *Digital Signature*	●	●	○	●	○	●
DCC	wanProvider *Digital Signature*	○	○	●	○	○	○

Other DCC Keys/Certificates that could be affected by a Compromise	
DCC	Root OCA Private Key / Certificate
DCC	Issuing OCA Private Key / Certificate
DCC	Contingency Symmetric Key
DCC	Contingency Private Key
DCC	Recovery Private Key / Certificate

Figure 1: Public Key Organisation Certificates / Keys covered by the SMKI Recovery Procedure

Figure 2, immediately below, shows the relevant Organisation Certificates that form the Device Security Credentials held by an S1SP for SMETS1Devices that are Commissioned within the DCC Systems:



		ESME electricity meter	GSME gas meter	CHF comms hub	GPF gas proxy	PPMID pre-payment meter
Supplier	Notified Critical Supplier Certificate	●	●	ESME Cert	●	ESME Cert
Supplier	Notified Non-Critical Supplier Certificate	●	●		●	
Network Operator	Notified Critical Network Operator Certificate	●			●	
Network Operator	Notified Non-Critical Network Operator Certificate	●			●	

Other DCC Keys/Certificates that could be affected by a Compromise	
DCC	Root OCA Private Key
DCC	Issuing CA Private Key

Figure 2: Organisation Certificates used by SMETS1 Service Providers for security credentials for SMETS1 Devices

The Check Cryptographic Protection applied by a SMETS1 Service Provider and the DCC to a Critical Service Request targeting a SMETS1 CHF or SMETS1 PPMID is carried out using the Notified Critical Supplier ID for the corresponding SMETS1 ESME.

2. Overview of the SMKI Recovery Procedure

In the event of an incident which:

a) results in the Compromise of a Relevant Private Key; or

b) causes the Subscriber for the Certificate associated with any of the Keys in a) above to reasonably suspect that there has been a Compromise of any such Key,

the provisions of this SMKI Recovery Procedure shall apply.

The SMKI Recovery Procedure includes procedures which detail the obligations of the DCC, Subscribers and the SMKI PMA, in respect of recovery from Compromise of a Relevant Private Key as set out in Section 1.2 of this document.

The table as set out immediately below summarises the actions required and the section(s) of this document which contain the applicable recovery procedure(s). It should be noted that it is possible to handle only one scenario type at a time and that there is a logical order of Section 4 first, then Section 6 second and then Section 5 last. This is to address the increasing severity of scenarios, their impact on the DCC Total System and the nature of the recovery procedure required. However, the execution of the steps is subject to SMKI PMA direction.

Compromise or Suspected Compromise of:	Section(s) of this document containing the procedure(s)
A Private Key which is associated with any Organisation Certificate, Data from which is used to populate the Device Security Credentials of a Device comprising part of an Enrolled Smart Metering System; or a Private Key which is associated with any Organisation Certificate, Data from which is used to populate part of any Device Security Credentials held by an S1SP	**4.1 Method 1 – recovery by the affected Subscriber using the Compromised Private Key (or any other relevant key held by the Subscriber)** to replace the associated Organisation Certificates on SMETS2+Devices 4.1.1 Pre-Recovery 4.1.2 Execution of Recovery Procedure 4.1.3 Post-Recovery **4.1A Method 1A – replacement of an Organisation Certificate forming part of S1SP Held Device Security Credentials** 4.1A.1Pre-Recovery 4.1A.2 Execution of Recovery Procedure 4.1A.3Post-Recovery **4.2 Method2 – recovery by the DCC using the Recovery Private Key to place DCC Access Control Broker Certificates on affected SMETS2+** Devices **(only available to a Supplier Party)** 4.2.1 Pre-Recovery 4.2.2 Execution of Recovery Procedure 4.2.3 Post-Recovery **Method 3 – recovery by the DCC using the Recovery Private Key to place new Organisation Certificates on SMETS2+ Devices**

	4.3.1 Pre-Recovery 4.3.2 Execution of Recovery Procedure 4.3.3 Post-Recovery

Root OCA Private Key	5.1 Pre-Recovery 5.2 Execution of Recovery Procedure 5.3 Post Recovery

Contingency Private Key or Contingency Symmetric Key	6.1.1 Pre-Recovery 6.1.2 Execution of Recovery Procedure 6.1.3 Post-Recovery

Recovery Private Key	6.2.1 Pre-Recovery 6.2.2 Execution of Recovery Procedure 6.2.3 Post-Recovery

Issuing OCA Private Key	6.3.1 Pre-Recovery 6.3.2 Execution of Recovery Procedure 6.3.3 Post-Recovery

Replacement of an XML Signing Private Key	7.1.1 XML Signing Private Key destruction considerations

3. General obligations

3.1 DCC Obligations

The DCC shall:

a) conduct the procedures set out in this document;

b) comply with any decisions made by the SMKI PMA regarding whether or not to take certain steps in order to recover from a Compromise;

c) where the DCC attempts but fails to replace one or more Organisation Certificates or OCA Certificates as part of operating these procedures, execute as many retries to replace such Organisation Certificates or OCA Certificates as the DCC can reasonably accommodate given the circumstances of the Compromise and capability of the DCC Systems, prior to any deadline for recovery as approved by the SMKI PMA;

d) where the DCC consults with the SMKI PMA regarding whether or not to take certain steps in order to recover from a Compromise and the DCC is directed such that recovery using the Recovery Private Key or Contingency Private Key should not be performed, the DCC shall inform all affected Parties of the outcome and any reasons provided by the SMKI PMA, as soon as reasonably practicable following such instruction, via a secured electronic means;

e) maintain confidential, auditable and secured records relating to the recovery from a Compromise, and the Devices and Subscribers affected by such Compromise; and

f) within three Working Days of the recovery from a Compromise, prepare a report regarding execution of the recovery and provide such report to the SMKI PMA, where such report shall include:

i. the process steps executed and the timing of the procedure to recover from the Compromise;

ii. where possible, carry out an analysis of which communications have been submitted to, or in relation to, any relevant affected Devices and any anomalous activity that should be investigated further by the DCC and/or affected Subscribers, and/or addressed via remedial actions; and

iii. keep this document under review and following consultation with the SMKI PMA, propose modifications to the SMKI Recovery Procedure that the DCC believes are necessary for the SMKI Recovery Procedure to meet the objectives more effectively as set out in the SEC.

Where such adjustments are needed to allow the effective executions of the procedures in this document, the DCC shall, as provided for in SEC Section L 10.2 (c), adjust the Anomaly Detection Thresholds, which it sets in other situations only after they are agreed by the Security Sub-Committee, subject only to the agreement of the SMKI PMA.

3.2 Notification and confirmation of a suspected Compromise

Any person may notify the DCC that there is a Compromise Relevant Private Key.

Where the DCC is notified or becomes aware of a Compromise Relevant Private Key, the DCC shall raise an Incident in accordance with sections 2.1 and 2.2 of the Incident Management Policy and shall notify the SMKI PMA, via secured electronic means, that a Compromise has been notified. The DCC shall contact the Subscriber for the Organisation Certificate associated with that Private Key or Contingency Symmetric Key (which may include the DCC itself as the Subscriber), as soon as reasonably practicable, via telephone and email using the contact details held by the SMKI Registration Authority. The DCC shall provide the Subscriber, via secured electronic means, with the appropriate Incident reference number and information relating to the notified Compromise. The DCC shall request confirmation from the Subscriber as to whether the Subscriber reasonably believes that a Compromise has occurred, and wishes to proceed with one or more of the recovery processes, which shall be confirmed by:

a) A SMKI Senior Responsible Officer (SMKI SRO) on behalf of a Party; or

b) A SMKI SRO, SMKI Registration Authority Manager or a member of SMKI Registration Authority Personnel authorised to act on behalf of the DCC in this capacity.

The Subscriber shall take reasonable steps to ensure that confirmation of whether it reasonably believes that a Compromise has occurred is provided to the DCC by the representatives above, within 24 hours of the request for confirmation from the DCC, via secured electronic means. Where the Subscriber confirms that it does not reasonably believe that a Compromise has occurred, the DCC shall close the Incident in accordance with section 2.12 of the Incident Management Policy.

Where the DCC receives confirmation that the Subscriber reasonably believes that a Compromise has occurred, the DCC shall also identify any Responsible Supplier(s) that are affected by the confirmed Compromise, in accordance with the procedures as set out in this document.

Where the DCC receives multiple Compromise notifications, the DCC may execute a common set of procedural steps to address such multiple Compromises, where it reasonably believes that such an approach would achieve the required recovery in an efficient manner.

3.3 Permitted mechanisms for confirmation of suspected Compromise

The DCC shall only accept the confirmation of a Compromise from a representative of the Subscriber as is defined in section 3.2 of this document, for an Organisation Certificate associated with a Compromised Private Key or from the DCC in respect of a Compromised Contingency Symmetric Key or the Compromise of an Organisation Certificate or OCA Certificate for which the DCC is the Subscriber, using the mechanisms as defined in the DCC's SMKI operational recovery procedures, which shall be made available by the DCC to Parties via secured electronic means.

3.4 Appointment and responsibilities of Key Custodians

The Organisation Certification Practice Statement (Organisation CPS) requires the Contingency Private Key and Recovery Private Key to be split into M#N Shares and that such Private Keys may be activated only via collaboration between appointed Key Custodians. The procedure as set out in this section 3.4 shall be followed in order to appoint such Key Custodians as are required.

3.4.1. Responsibilities in respect of Key Custodians

Each Party, the DCC, the SMKI PMA or the Panel, on behalf of which an individual acting on behalf of that organisation becomes a Key Custodian, shall ensure that the Key Custodian:

a) does not seek to find out the identity of other Key Custodians or otherwise collude with other Key Custodians in relation to matters associated with this Recovery Procedure other than for the purposes as set out in this SMKI Recovery Procedure;

b) does not disclose the fact that they are a Key Custodian, other than:

   i. in the case of each Party, to a Director, Company Secretary, SMKI SRO or Chief Information Security Officer for the organisation they represent; or

   ii. in the case of the SMKI PMA or Panel, to other members of the SMKI PMA or Panel; and

   iii. to those other persons to whom the information reasonably needs to be disclosed for reasons of personnel management within the relevant organisation, and furthermore shall ensure that persons within their organisation who are aware of the identity of a Key Custodian shall not disclose the identity of a Key Custodian more widely;

c) takes all reasonable steps to protect and not to lose any safety deposit box key issued to them to secure any Cryptographic Module as part of the relevant Key Generation Ceremony, and which is used by the Key Custodian to secure the Cryptographic Module containing the Key Component issued to them, in accordance with any guidance documentation provided by the DCC to the Key Custodian via secured electronic means;

d) where the safety deposit box securing the Cryptographic Module containing a Key Component cannot be accessed, or the safety deposit key is lost or cannot be accessed, the DCC shall raise an Incident in accordance with sections 2.1 and 2.2 of the Incident Management Policy and shall take such steps as are necessary to resolve the Incident;

e) takes all reasonable steps to attend a Key Generation Ceremony or Key Activation Ceremony when requested by the DCC and, where they are to attend, to take all steps that are reasonably practical to attend at the time requested by the DCC; and

f) is, upon request to attend a Key Generation Ceremony or Key Activation Ceremony by the DCC, immediately released to perform the Key Custodian role unless it would be materially disruptive to the business of the relevant organisation for them not to be released at that time.

Where a Party is the Subscriber for an Organisation Certificate that is Compromised (or is suspected to be Compromised), the Subscriber is not the DCC and an individual acting on behalf of that Subscriber is a Key Custodian; the DCC may exclude that Key Custodian from attending any Key Generation Ceremony or Key Activation Ceremony required as part of the applicable recovery procedure, where the DCC considers such action to be appropriate to mitigate security risks. If such exclusion occurs, the DCC shall record the decision made, and shall notify that Key Custodian and a SMKI SRO for the Subscriber, via secured electronic means.

3.4.2. Ceasing to be a Key Custodian

In the event that a Party, the DCC, the SMKI PMA or the Panel wishes a particular individual to cease their role as a Key Custodian:

a) such Party, the SMKI PMA or the Panel shall notify the DCC in writing, at least one month in advance of the date on which that it wishes the individual acting as a Key Custodian to cease to be a Key Custodian;

b) the relevant Party, the DCC, the SMKI PMA or the Panel shall arrange for the Key Custodian to return the physical key for the corresponding safety deposit box in which the Cryptographic Module containing the relevant Key Component is held, to a Registration Authority Manager at the DCC's address as published on the DCC Website, by secure courier;

c) the DCC shall update its records of Key Custodians; and

d) the DCC shall conduct, insofar as necessary, the procedure as set out in section 3.4.3 immediately below.

3.4.3. Detailed procedure for appointment of Key Custodians

The procedure as set out immediately below shall be executed by the DCC, Parties, the SMKI PMA and the Panel in order to appoint Key Custodians.

Step	When	Obligation	Responsibility	Next Step
3.4.3.1	As identified by the DCC that Key Custodians are required	The DCC shall identify the need for Key Custodians in respect of a Recovery Private Key or Contingency Private Key.	DCC	3.4.3.2
3.4.3.2	As soon as reasonably practicable, following 3.4.3.1	The DCC shall issue a request for nominations, via a secured electronic means, to Parties, the DCC, the SMKI PMA and the Panel, for individuals to become Key Custodians for the Recovery Private Key or Contingency Private Key	DCC	3.4.3.3

		as identified in step 3.4.3.1. Such request for nominations shall: a. include the Key Custodian nomination form as published on the DCC Website; b. be marked as confidential; and c. detail the locations where each relevant Key Generation Ceremony and any corresponding Key Activation Ceremony will take place.		

3.4.3.3	Within 10 Working Days of the issuance of the request for nominations	Each Party, the DCC, the SMKI PMA or the Panel wishing to nominate an individual to become a Key Custodian in respect of a particular Private Key shall provide, via secured electronic means, to the DCC for each nominated individual, a completed Key Custodian nomination form using the pro-forma as published on the DCC Website. The nomination form should contain the following information: a. the full name of a Director, Company Secretary or SMKI Senior Responsible Officer who is nominating the individual to become a Key Custodian for a Party, the DCC, the SMKI PMA Chair for the SMKI PMA or the Panel Chair for the Panel; b. the full name of the nominated individual; c. contact telephone details for the nominated individual; d. the nominated individual's normal work location; e. the estimated time to travel to the location of the relevant Key Generation Ceremony and to the location of the corresponding Key Activation Ceremony, as notified in step 3.4.2; f. evidence that the individual is: i. for a Party, an employee or Director of the Party; ii. for the DCC, an employee of the DCC or a DCC Service Provider; iii. for the SMKI PMA, an appointed member of the SMKI PMA; or iv. for the Panel, an appointed member of the Panel; and g. evidence that the nominated individual has successfully completed security screening in a manner that is compliant with: i. British Standard BS 7858:2012 (Security Screening of Individuals Employed in a Security Environment –	Party, DCC, the SMKI PMA or the Panel	3.4.3.4

		Code of Practice); or ii. any equivalent to that British Standard which updates or replaces it from time to time. Where necessary in order to have a sufficient number of Key Custodians appointed, the SMKI PMA may direct any Party to nominate individuals to become Key Custodians. Where this occurs, the directed Party shall identify and nominate individuals in accordance with this step 3.4.3.3.		
3.4.3.4	As soon as reasonably practicable following 3.4.3.3	The DCC shall determine: a. using publicly available information, whether the Director, Company Secretary, SMKI Senior Responsible Officer, SMKI PMA Chair or Panel Chair who is nominating the individual to become a Key Custodian holds such a role on behalf of the organisation; and b. whether the information supplied in the Key Custodian nomination form is complete and accurate. Where there are omissions/discrepancies, agree actions with the nominating Director, Company Secretary, SMKI Senior Responsible Officer, SMKI PMA Chair or Panel Chair, via secured electronic means or in writing.	DCC	If complete, 3.4.3.5; if not complete, 3.4.3.3
3.4.3.5	As soon as reasonably practicable, following 10 Working Days after issuance of request for nominations	The DCC shall collate nominations received and shall provide to SMKI PMA: a. details of those nominated individuals and the organisation they are representing; and b. upon request from the SMKI PMA, details held by the DCC of all existing holders of Key Components.	DCC	3.4.3.6
3.4.3.6	As soon as reasonably practicable, following 3.4.3.5	The SMKI PMA shall determine the individuals that shall become Key Custodians, which shall take into account geographical location and how many Key Components are held by any particular organisation or individual (where relevant). The SMKI PMA shall inform the DCC of the individuals which shall become Key Custodians.	SMKI PMA	3.4.3.7 if sufficient Key Custodians can be appointed; if not, 3.4.3.3
3.4.3.7	As soon as reasonably	The DCC shall confirm that the individual has been	DCC	3.4.3.8

	practicable, following 3.4.3.6	selected by the SMKI PMA to become a Key Custodian and shall confirm the date and time for a verification meeting for the nominated individual at the DCC's offices, to the Director, Company Secretary, SMKI Senior Responsible Officer, SMKI PMA Chair or Panel Chair of the applicant organisation who nominated the individual to become a Key Custodian, via secured electronic means.		
3.4.3.8	At verification meeting	The DCC shall, in person, verify the individual identity of the nominated individual to the level pursuant to the SMKI PMA Guidance on 'Verifying Individual Identity' published on the Website.	DCC	If successful for all, 3.4.3.10; for unsuccessful, 3.4.3.9
3.4.3.9	As soon as reasonably practicable following rejection	The DCC shall notify the nominating Director, Company Secretary, SMKI PMA Chair or Panel Chair, in writing, that the nominated individual could not at that point be appointed as a Key Custodian.	DCC	3.4.3.6
3.4.3.10	As soon as reasonably practicable, following 3.4.3.8	The DCC shall notify, in writing via secured electronic means: a. the individual, in person, that they are eligible to become a Key Custodian; and	DCC	3.4.3.11

		b. the nominating Director, Company Secretary, SMKI PMA Chair or Panel Chair, that the nominated individual is eligible to become a Key Custodian.		
3.4.3.11	As soon as reasonably practicable, following 3.4.3.10	The DCC shall: a. update its records of eligible Key Custodians for Private Keys for which Key Components are issued and shall store such records in a secured manner; and b. inform the SMKI PMA Chair, in writing, that the nominated individual has become a Key Custodian	DCC	Relevant procedure to recover from a notified Compromise

3.5 Recovery Actions Risk

3.5.1 Actions to be taken only after considering Recovery Action Risks

The actions detailed in this section 3.5.1 shall only be taken when those identified, in this document, as responsible for decision making have considered the risks detailed in sections 3.5.2 and 3.5.3 ('Recovery Action Risks'), and either concluded that they are not relevant or that, on balance, the risks of taking the actions are less than the risks of not taking them, having factored in any mitigations that have been, or are being, put in place. The timing of any such actions may therefore be delayed to a later time, including to ensure that mitigations are in place.

Such consideration shall factor in the risk that a Compromised Private Key may, depending on the Compromise, be used to send unauthorised instructions to the corresponding fleet of Devices, until the associated Certificates on SMETS2+ Devices have been replaced and also revoked (so that DCC systems will no longer accept their use).

The actions to be considered prior to a decision to undertake SMKI Recovery are:

- Any action that would lead to one or more Devices having their SMI status set to 'Recovery';
- The revocation of a Certificate;
- The destruction of a Private Key (or any other action that would render it unusable); or
- The placing of Access Control Broker Certificates in Supplier Trust Anchor Cells on a SMETS2+ Device, and therefore any request to use 'Method 2', with its section 4.2 meaning.

3.5.2 Prepayment functionality and continuity of Supply to the Consumer

Where a capitalised term in this section is not defined either in this document or in SEC Section A, that term shall have its SMETS meaning.

All SMETS ESME and GSME have the ability to operate in Prepayment Mode, a feature of which is that, when there is insufficient credit, Supply to the Premises will be Disabled. To ensure continuity of supply in recovering from a Compromise, it is important either that supplier prepayment functions can continue to operate during the recovery, or that the potentially affected ESME and/or GSME are placed in a state where they will not Disable

Supply during the recovery. For example, this could be achieved by switching such Devices to Credit mode and then locking out supplier functionality until recovery is complete.

Whilst the technical security mechanisms (and so potential effects of recovery actions) vary somewhat between SMETS1 and SMETS2+, the recovery actions that may affect operation in Prepayment Mode include:

- Destruction of XML Signing Private Keys, where they are used to sign Service Requests for prepayment functions, or revocation of associated Certificates. In the absence of replacements, this would mean all prepayment functionality, other the locally entered SMETS2+ top ups, would be lost;

- Destruction of supplier Private Keys, where they are used to sign Commands to SMETS2+ Devices. In the absence of a replacement, this would mean all SMETS2+ prepayment functionality, other the locally entered SMETS2+ top ups, would be lost. It is important to note that revocation of the associated supplier Certificates does NOT stop the supplier Private Keys being used to instruct SMETS2+ Devices;

- Destruction of supplier Private Keys, where they are used to create SMETS2+ top ups. In the absence of a replacement, and the corresponding update of supplier related Device Security Credentials (i.e. certificate information) on SMETS2+ Devices, this would prevent SMETS 2+ top ups. It is important to note that revocation of the associated supplier Certificates does NOT stop the supplier Private Keys being used to instruct SMETS2+ Devices;

- Replacement of supplier credentials on SMETS2+ Devices with Access Control Broker credentials. This locks out all supplier prepayment functionality on the Device, until the Access Control Broker credentials have subsequently successfully been replaced with valid supplier credentials;

- Revocation of Certificates associated with XML Signing Private Keys, which means that those Private Keys can no longer be used to sign XML needed to deliver prepayment functionality; and

- Setting the SMI Status of a Smart Meter to 'Recovery' which blocks prepayment functionality delivered via the DCC.

An important factor to consider is therefore the number of ESME and/or GSME that could be affected by the Compromise and are understood to currently be in Prepayment mode. However, it is important to note that certain Compromises could, in theory, allow Devices to be switched to Prepayment Mode without supplier authorisation. In such cases, the speed at which that potential risk is removed should also be factored in.

3.5.3 Devices in the supply chain

Where a capitalised term in this section is not defined either in this document or in SEC Section A, that term shall have its GBCS meaning.

To enforce end-to-end security, the SEC requires that SMETS2+ Devices have the range of security credentials, detailed in Figure 1, recorded in the Device's Trust Anchor Cells before installation. To that end, the DCC makes available a set of the following Certificates for loading on to Devices before installation. The relevant Certificates must be recorded on Devices before they are installed, otherwise enduring communications will not be possible:

- Root Certificate;

- Recovery Certificate;

- CoS Certificate; and

- Access Control Broker Certificates (one with a key usage of key agreement, and the other with a key usage of digital signature).

Additionally:

- Communications Hub Functions must hold information from a WAN Provider Certificate.
- ESME and GSME may hold information from Supplier Certificates, although information from Access Control Broker Certificates can be used in the Supplier and Network Operator Trust Anchor Cells.

Should any of the associated Private Keys (including the Contingency Private Key) be destroyed or made unusable as part of a recovery process, then it may no longer be possible to Commission Devices still in the supply chain, or such Commissioning may require keeping the Recovery or Contingency Private Key in extended operation, with the risks that brings.

In light of the potential economic costs and logistical disruption to the maintenance of metering, careful consideration should therefore be given to the destruction, or making inoperable, of any such Private Keys.

After a Recovery Event as described in Section 6, all supply chain Devices will still be able to be Commissioned and used by being updated to the new Root OCA Certificate in a future Recovery Event to restore the capabilities described in Section 6.

4. Procedure to recover from the Compromise of a Private Key corresponding with a Public Key contained within an Organisation Certificate held on a SMETS2+ Device (other than the Recovery Private Key); or which forms part of any S1SP Held Device Security Credentials

This section sets out the procedures that may be used in order to recover from the Compromise of a Private Key associated with an Organisation Certificate held on a SMETS2+ Device (other than the Recovery Private Key), or to replace Organisation Certificates forming part of any S1SP Held Device Security Credentials where a Subscriber wishes to recover from the Compromise using this procedure.

Where a Subscriber wishes to recover from the Compromise of such a Private Key and its associated Public Key contained within the Organisation Certificate using any of the methods listed immediately below, it shall notify the DCC of which of the methods listed immediately below that it wishes to use, using the mechanisms as defined in the DCC's SMKI operational recovery procedures, which shall be made available by the DCC to Parties via secured electronic means. The DCC shall update the Incident Management Log to record such notification in accordance with H9.1(g).

a) **Method 1:** the Subscriber shall seek to recover using the Compromised (or one suspected of being Compromised) Private Key (or any other relevant key held by the Subscriber) to replace the associated Organisation Certificate to which the Relevant Private Key relates on all affected SMETS2+ Devices;

b) **Method 1A:** the Subscriber shall seek to recover using the Compromised (or one suspected of being Compromised) Private Key (or any other relevant key held by the Subscriber) to replace all affected S1SP Held Device Security Credentials to which the Relevant Private Key relates;

c) **Method 2:** (only applicable where the Subscriber is a Supplier Party), the DCC shall use the Recovery Private Key to replace affected Certificates on SMETS2+ Devices with a DCC Access Control Broker

Certificate. The Responsible Supplier shall then complete the recovery process by replacing the DCC Access Control Broker Certificate with new Organisation Certificates for which it is the Subscriber; or

d) **Method 3:** the DCC shall recover using the Recovery Private Key to replace affected Organisation Certificates on SMETS2+ Devices with new Organisation Certificates provided by the Subscriber.

Following the notification of the selected recovery method by the Subscriber, the DCC shall:

e) Where method 1 has been selected, perform the procedure as set out in Section 4.1 of this document;

f) Where method 1A is being used, perform the procedure as set out in Section 4.1A of this document;

g) Where method 2 has been selected, perform the procedure as set out in Section 4.2 of this document; or

h) Where method 3 has been selected, perform the procedure as set out in Section 4.3 of this document.

4.1 Method 1 - recovery by the affected Subscriber using the Compromised Private Key (or any other relevant key held by the Subscriber) to replace the associated Organisation Certificates on SMETS2+ Devices

4.1.1 Pre-Recovery

The DCC shall execute the procedure as set out immediately below, following notification of the Compromise of the Private Key associated with the Public Key contained within an Organisation Certificate held on a SMETS2+ Devices, in accordance with section 3.2 of this document and notification from the affected Subscriber that it wishes to recover from the Compromise using the procedure set out in this section.

Informative:

Where the Compromised Private Key is a supplier Private Key, there are two ways in which the Subscriber (the supplier) can, using Private Keys it controls, effect replacement of the associated Certificates. Specifically, it can use either of the two mechanisms provided for in DUIS:

- Update Security Credentials (KRP) (SRV 6.15.1) or

- Update Security Credentials (CoS) (SRV 6.23)

The ‘CoS’ mechanism will work regardless of the state of the supplier Digital Signature Private Key (so the key used to sign Commands to Devices), and so may have advantages in some scenarios, including in its allowing earlier destruction of any Compromised supplier Digital Signature Private Key.

Thus, in the scenario where the Compromised Private Key is a supplier Private Key, the Subscriber should always consider both DUIS options and factor that consideration in to assessing how best to recover from the Compromise.

- This section does not apply to XML Signing Private Keys. Please see Section 7 of this document for further guidance on the XML Signing Private Keys.
- This section is only applicable to Responsible Suppliers, Electricity Distributors, Gas Transporters and the DCC.

Step	When	Obligation	Responsibility	Next Step
4.1.1.1	As soon as possible, following notification that the Subscriber wishes to recover using its own Compromised (or one suspected of being Compromised) Private Key associated with the Public Key contained within an Organisation Certificate held on a SMETS2+ Device	The affected Subscriber shall consider the Recovery Action Risks before undertaking any of the associated actions. If the Private Key is not operable at this stage, the affected Subscriber should first consider using other Private Keys that it controls to affect the recovery. Specifically, if the Subscriber is a Supplier Party it should consider using other Private Keys to invoke Update Security Credentials (CoS) (SRV 6.23) Service Requests as the certificate replacement method (including factoring in that this would not block prepayment functionality and would allow certificate replacement to Devices in the supply chain). If such methods are considered not viable or sufficient, the Subscriber should follow the Recovery Procedure as laid out in Section 4.2, Method 2 - recovery by the DCC using the Recovery Private Key to place DCC Access Control Broker Certificates on affected SMETS2+ Devices.	Subscriber	4.1.1.2 or 4.2
4.1.1.2	As soon as reasonably practicable, following 4.1.1.1	A SMKI ARO acting on behalf of the affected Subscriber shall submit to the DCC, via secured electronic means, one or more files which shall be Organisation Compromise Notification Files as set out in Appendix B for Subscribers that are not the DCC, or Other Compromise Notification Files as set out in Appendix D where the Subscriber is the DCC. The affected Subscriber should ensure that such files together contain details of: a. the Incident to which the submission relates; b. the EUI-64 identifiers for the organisation that is the affected Subscriber to which the Compromise, or suspected Compromise of the Private Key relates; and c. for each Organisation Certificate that is affected by the Compromise of the associated Private Key, the serial number of the Organisation Certificate, the SMETS2+ Device IDs and the SMETS2+ Device Trust Anchor Cell which is populated with the affected Organisation Certificate related to the Compromised (or one suspected of being Compromised) Private Key.	Subscriber	4.1.1.3

		In addition, a SMKI ARO acting on behalf of the affected Subscriber shall, as soon as reasonably practicable, submit an Anomaly Detection Thresholds File to the DCC, which shall include amended Anomaly Detection Thresholds that they estimate will be required to replace all affected Organisation Certificates on SMETS2+ Devices. The affected Subscriber shall ensure that the Anomaly Detection Thresholds File is submitted in accordance with the provisions of the TADP.		

4.1.1.3	As soon as reasonably practicable, following 4.1.1.2	The DCC shall notify the SMKI PMA, via a secured electronic means, as soon as reasonably practicable: a. that a Compromise of an Organisation's Private Key has been notified; b. that the Subscriber intends to use method 1 (as set out in section 4.1 of this document) to recover; c. which of the two sub-options that the Subscriber intends to use (i.e. Update Security Credentials (KRP) (SRV 6.15.1) or Update Security Credentials (Co S) (SRV 6.23) or a combination of the two); d. of details relating to the Compromise, comprising the	DCC	4.1.1.4

		Subscriber and the number of SMETS2+ Devices affected, which will include the Organisation Compromise Notification Files as set out in Appendix B for Subscribers that are not the DCC, or Other Compromise Notification Files as set out in Appendix D where the Subscriber is the DCC; and e. of recommendations for any amendments to the Anomaly Detection Thresholds set by the DCC under SEC Section G6.		

4.1.1.4	As soon as reasonably practicable, following 4.1.1.3	Where the affected Subscriber is not the Responsible Supplier for a SMETS2+ Device that is notified in step 4.1.1.1, the DCC shall notify the Responsible Supplier, via secured electronic means, that a Subscriber wishes to recover from Compromise using its own Private Key. The DCC shall also provide to the Responsible Supplier, via a secured electronic means, one or more Organisation Compromise Notification Files as set out in Appendix B for Subscribers that are not the DCC, or Other Compromise Notification Files as set out in Appendix D where the Subscriber is the DCC, which together contain details of the SMETS2+ Device IDs to which the Compromise relates.	DCC	Procedure as set out in section 4.1.2 of this document

4.1.2 Execution of Recovery Procedure

The procedure as set out immediately below, amended as instructed by the SMKI PMA, shall be used following execution of the process as set out in section 4.1.1 of this document except for 4.1.2.6 which may be undertaken at any time that is decided in accordance with these.

Step	When	Obligation	Responsibility	Next Step
4.1.2.1	As soon as reasonably practicable, following procedure as set out in section 4.1.1	The DCC shall apply the amended Anomaly Detection Thresholds for the affected Subscriber in accordance with the TADP. The DCC shall inform, via a secured electronic means, a SMKI SRO and the SMKI ARO that provided the details in step 4.1.1.2, that the Anomaly Detection Threshold values have been successfully amended. In respect of the Anomaly Detection Thresholds set by the DCC under SEC Section G6, if amendments are agreed by the SMKI PMA, the DCC shall apply the amended Anomaly Detection Thresholds in accordance with the TADP.	DCC (DSP TAD)	4.1.2.2
4.1.2.2	As soon as reasonably practicable, following 4.1.2.1	The affected Subscriber shall either: a. identify replacement Organisation Certificates; or b. submit such Certificate Signing Requests (CSRs) that are required in order to acquire new Organisation Certificates.	Subscriber	4.1.2.3
4.1.2.3	As soon as reasonably practicable,	The affected Subscriber shall submit Service Requests as required, in accordance with the provisions of the DCC User Interface Specification,	Subscriber	4.1.2.4

	following 4.1.2.2	to replace affected Organisation Certificates on all relevant SMETS2+ Devices and shall, in doing so, monitor replacement of such affected Organisation Certificates.		
4.1.2.4	As soon as reasonably practicable, following 4.1.2.3	Upon completion of its activities to replace affected Organisation Certificates on affected SMETS2+ Devices, the affected Subscriber shall inform the DCC, via a secured electronic means: a. that its activities in respect of the replacement of Organisation Certificates have been completed; and b. of the SMETS2+ Devices for which replacement of affected Organisation Certificates has not been completed, which shall be submitted as one or more Organisation Compromise Recovery Progress Files as set out in Appendix C for Subscribers that are not the DCC, or Other Compromise Recovery Progress Files as set out in Appendix E.	Subscriber	4.1.2.6 or 4.1.2.5 if appropriate
4.1.2.5	As soon as reasonably practicable, following 4.1.2.4	Where the affected Subscriber is not the Responsible Supplier for a SMETS2+ Device that is notified in step 4.1.1.1, the DCC shall notify the Responsible Supplier for affected SMETS2+ Devices, via secured electronic means, which SMETS2+ Devices were not recovered successfully, in one or more Organisation Recovery Progress Files as set out in Appendix C for Subscribers that are not the DCC, or Other Compromise Recovery Progress Files as set out in Appendix E where the Subscriber is the DCC.	DCC	Procedure as set out in section 4.1.2.6 of this document
4.1.2.6	As decided after considering the Recovery Action Risks	The affected Subscriber shall consider the Recovery Action Risks before undertaking any of the associated actions. Where the Subscriber concludes that, at this time, Certificates should not be revoked and / or Private Keys not destroyed, the Subscriber shall inform the SMKI PMA as to the rationale. The affected Subscriber may, having considered the Recovery Action Risks, submit Certificate Revocation Requests (CRRs), as set out in the SMKI RAPP, in order to revoke affected Organisation Certificates. The DCC shall revoke Organisation Certificates in accordance with the provisions of Appendix B of the Code and the SMKI RAPP section 8.2. The affected Subscriber may, having considered the	Subscriber, DCC	Procedure as set out in section 4.1.3 of this document

		Recovery Action Risks, destroy the Private Key associated with the revoked Organisation Certificates.		

4.1.3 Post-Recovery

The procedure as set out immediately below shall be used following recovery from the Compromise of a Private Key associated with an Organisation Certificate using the procedures as set out in sections 4.1.1 and 4.1.2 of this document.

Step	When	Obligation	Responsibility	Next Step
4.1.3.1	As soon as reasonably practicable, following completion of the procedure as set out in Section 4.1.2 of this document	A SMKI ARO acting on behalf of the affected Subscriber shall, as soon as reasonably practicable, submit appropriate enduring Anomaly Detection Thresholds to the DCC, in accordance with the TADP. The DCC shall amend the relevant Anomaly Detection Thresholds in accordance with the TADP.	DCC (DSP TAD)	4.1.3.2
4.1.3.2	As soon as reasonably practicable, following 4.1.3.1	The DCC shall notify the SMKI PMA via a secured means of: a. the completion of the affected Subscriber's activities in respect of the procedure as set out in this section 4.1; and b. the SMETS2+ Devices for which recovery was not completed, which may be provided in one or more which shall be Organisation Compromise Recovery Progress Files as set out in Appendix C for Subscribers that are not the DCC, or Other Compromise Recovery Progress Files as set out in Appendix E where the Subscriber is the DCC.	DCC	End of procedure

4.1A Method 1A – replacement by the affected Subscriber using its Compromised Private Key of associated S1SP Held Device Security Credentials

4.1A.1 Pre-Recovery

The DCC shall execute the procedure as set out immediately below, following notification of the Compromise of the Private Key associated with the Public Key contained within an Organisation Certificate that forms a part of any S1SP Held Device Security Credentials, in accordance with section 3.2 of this document and notification from the affected Subscriber that it wishes to recover from the Compromise using the procedure set out in this section.

Informative:

- Please see Section 7 of this document for further guidance on the XML Signing Private Keys.
- This section is only applicable to Responsible Suppliers, Electricity Distributors and Gas Transporters.
- All S1SP Held Device Security Credentials are Organisation Certificates.
- S1SP Held Device Security Credentials are held by the SMETS1 Service Provider and not on the SMETS1 Device.

Step	When	Obligation	Responsibility	Next Step
4.1A. 1.1	As soon as possible, following notification that the Subscriber wishes to recover using its own Compromised (or one suspected of being Compromised) Private Key associated with the Public Key contained within an Organisation Certificate that forms part of any S1SP Held Device Security Credentials	The affected Subscriber shall consider the security risks arising from the Compromise of its Private Key and be aware that, until the Private Key is destroyed, there is a risk of the Private Key being used to achieve adverse consequences for the consumer. Revoking the Organisation Certificate (that forms part of any S1SP Held Device Security Credentials) containing the Public Key associated with the Compromised (or one suspected of being Compromised) Private Key will prevent the Private Key from being used to send authorised Commands to a SMETS1 Device. Due consideration should be given before destroying a Compromised (or one suspected of being Compromised) Private Key if the recovery steps detailed in 4.1A.2.1 to 4.1A.2.5 of this section have not yet been carried out. Destroying the Private Key prior to carrying out these steps may put pre-payment customers at risk. It would be advisable to conduct the replacement of Organisation Certificates that forms part of any S1SP Held Device Security Credentials as quickly as possible.	Subscriber	4.1A.1.2

4.1A.1.2	As soon as reasonably practicable, following 4.1A.1.1	A SMKI ARO acting on behalf of the affected Subscriber shall submit to the DCC, via secured electronic means, one or more files which shall be Organisation Compromise Notification Files as set out in Appendix B. The affected Subscriber should ensure that such files together contain details of: a. the Incident to which the submission relates; b. the EUI-64 identifiers for the organisation that is the affected Subscriber to which the Compromise, or suspected Compromise of the Private Key relates; and c. for each Organisation Certificate that forms part of any S1SP Held Device Security Credentials and is affected by the Compromise, the serial number of the Organisation Certificate, the SMETS1 Device IDs and the nature of the affected S1SP Held Device Security Credentials. In addition, a SMKI ARO acting on behalf of the affected Subscriber shall, as soon as reasonably practicable, submit an Anomaly Detection Thresholds File to the DCC, which shall include amended Anomaly Detection Thresholds that they estimate will be required to replace the affected Organisation Certificates that form a part of any S1SP Held Device Security Credentials. The affected Subscriber shall ensure that the Anomaly Detection Thresholds File submitted in accordance with the TADP.	Subscriber	4.1A.1.3
4.1A.1.3	As soon as reasonably practicable, following 4.1A.1.2	The DCC shall notify the SMKI PMA, via a secured electronic means, as soon as reasonably practicable: a. that a Compromise of an Organisation's Private Key has been notified; b. that the Subscriber intends to use method 1 (as set out in section 4.1A of this document) to recover; and c. of details relating to the Compromise, comprising the Subscriber and the number of Organisation Certificates that form a part of any S1SP Held Device Security Credentials affected, which will include the Organisation Compromise Notification Files as set out in Appendix B for Subscribers that are not the DCC, or Other	DCC	4.1A.1.4

		Compromise Notification Files as set out in Appendix D where the Subscriber is the DCC.		

4.1A.2 Execution of Recovery Procedure

The procedure as set out immediately below, amended as instructed by the SMKI PMA, shall be used following execution of the process as set out in section 4.1A.1 of this document, except for 4.1.A.2.6 which may be undertaken at any time that is decided in accordance with these.

Step	When	Obligation	Responsibility	Next Step
4.1A .2.1	As soon as reasonably practicable, following procedure as set out in section 4.1A.1	The DCC shall amend the Anomaly Detection Thresholds for the affected Subscriber in accordance with the TADP. The DCC shall inform, via a secured electronic means, a SMKI SRO and the SMKI ARO that provided the details in step 4.1A.1.2, that the Anomaly Detection Threshold values have been successfully amended.	DCC (DSP TAD)	4.1A.2.2
4.1A. 2.2	As soon as reasonably practicable, following 4.1A.2.1	The affected Subscriber shall either: a) identify replacement Organisation Certificates that form a part of any S1SP Held Device Security Credentials; or b) submit such Certificate Signing Requests (CSRs) that are required in order to acquire new Organisation Certificates that form a part of any S1SP Held Device Security Credentials.	Subscriber	4.1A.2.3
4.1A. 2.3	As soon as reasonably practicable, following 4.1A.2.2	The affected Subscriber shall submit Service Requests as required, in accordance with the provisions of the DCC User Interface Specification, to replace affected Organisation Certificates that form a part of any S1SP Held Device Security Credentials and shall, in doing so, monitor replacement of such affected Organisation Certificates.	Subscriber	4.1A.2.4
4.1A. 2.4	As soon as reasonably practicable, following 4.1A.2.3	Upon completion of its activities to replace affected Organisation Certificates that form a part of any S1SP Held Device Security Credentials, the affected Subscriber shall inform the DCC, via a secured electronic means: a) that its activities in respect of the replacement of Organisation Certificates that form a part of any S1SP Held Device Security Credentials have been completed; and b) of the Organisation Certificates that form a part	Subscriber	4.1A.2.6 or 4.1A.2.5 if appropriate

		of any S1SP Held Device Security Credentials for which replacement has not been completed, which shall be submitted as one or more Organisation Compromise Recovery Progress Files as set out in Appendix C for Subscribers that are not the DCC, or Other Compromise Recovery Progress Files as set out in Appendix E.		
4.1A. 2.5	As soon as reasonably practicable, following 4.1A.2.4	Where the affected Subscriber is not the Responsible Supplier for a SMETS1 Device that is notified in step 4.1A.1.1, the DCC shall notify the Responsible Supplier for affected SMETS1 Devices, via secured electronic means, which SMETS1 Devices were not recovered successfully, in one or more Organisation Recovery Progress Files as set out in Appendix C for Subscribers that are not the DCC, or Other Compromise Recovery Progress Files as set out in Appendix E where the Subscriber is the DCC.	DCC	Procedure as set out in section 4.1A.2.6 of this document
4.1 A.2. 6	As decided following consideration of the Recovery Action Risks, following 4.1A.2.4	The affected Subscriber shall consider the Recovery Action Risks before undertaking any of the associated actions. Where the Subscriber concludes that, at this time, Certificates should not be revoked and / or Private Keys not destroyed, the Subscriber shall inform the SMKI PMA as to the rationale. The affected Subscriber may, having considered the Recovery Action Risks, submit Certificate Revocation Requests (CRRs), as set out in the SMKI RAPP, in order to revoke affected Organisation Certificates that form a part of any S1SP Held Device Security Credentials. The DCC shall revoke Organisation Certificates that form a part of any S1SP Held Device Security Credentials in accordance with the provisions of Appendix B of the Code and the SMKI RAPP. The affected Subscriber may, having considered the Recovery Action Risks, destroy the Private Key associated with the revoked Organisation Certificate that forms a part of any S1SP Held Device Security Credentials.	Subscriber, DCC	Procedure as set out in section 4.1A.3 of this document

4.1A.3 Post-Recovery

The procedure as set out immediately below shall be used following recovery from the Compromise of a Private Key associated with an Organisation Certificate using the procedures as set out in sections 4.1A.1 and 4.1A.2 of this document.

Step	When	Obligation	Responsibility	Next step
4.1A.3.1	As soon as reasonably practicable, following completion of the procedure as set out in Section 4.1A.2 of this document	A SMKI ARO acting on behalf of the affected Subscriber shall, as soon as reasonably practicable, submit appropriate enduring Anomaly Detection Thresholds to the DCC, in accordance with the TADP. The DCC shall amend the relevant Anomaly Detection Thresholds in accordance with in the TADP.	DCC (DSP TAD)	4.1A.3.2
4.1A.3.2	As soon as reasonably practicable, following 4.1A.3.1	The DCC shall notify the SMKI PMA via a secured means of: a. the completion of the affected Subscriber's activities in respect of the procedure as set out in this section 4.1A; and b. the Organisation Certificates that form a part of any S1SP Held Device Security Credentials for which recovery was not completed, which may be provided in one or more which shall be Organisation Compromise Recovery Progress Files as set out in Appendix C for Subscribers that are not the DCC, or Other Compromise Recovery Progress Files as set out in Appendix E where the Subscriber is the DCC.	DCC	End of procedure

4.2. Method 2 - recovery by the DCC using the Recovery Private Key to place DCC Access Control Broker Certificates on affected SMETS2+ Devices

4.2.1 Pre-Recovery

The DCC shall execute the procedure as set out immediately below, following notification of the Compromise of the Private Key associated with the Public Key contained within an Organisation Certificate, in accordance with section 3.2 of this document, and notification from the affected Subscriber that it wishes to recover from the Compromise using the procedure set out in this section.

The affected Subscriber shall only request use of the procedure in this section having considered the Recovery Action Risks, including that section 4.2.1.3 requires the DCC to disable access, via the DCC, to affected Devices **before the SMKI PMA has reached a decision as to whether to proceed**. For clarity, this includes disablement of all prepayment functionality operated via the DCC.

Step	When	Obligation	Responsibility	Next Step
4.2.1.1	As soon as possible, following notification that the Subscriber wishes to recover using the procedure set out in section 4.2 of this document	The affected Subscriber should not take any action, prior to the SMKI PMA making a decision as to whether to use this procedure, that would prejudge that outcome unless they consider risks are sufficient to justify such advance actions. For clarity, this includes the actions to which Recovery Action Risks relate.	Subscriber, DCC	4.2.1.2
4.2.1.2	As soon as possible, following 4.2.1.1	A SMKI ARO acting on behalf of the affected Subscriber shall submit to the DCC, via secured electronic means, one or more Organisation Compromise Notification Files that each comply with Appendix B of this document and which together contain details of: a) the Incident to which the submission relates; b) the EUI-64 identifiers for the organisation that is the affected Subscriber to which the Compromise, or suspected Compromise relates; and c) for each Organisation Certificate that is affected by the Compromise, the serial number of the Organisation Certificate, the SMETS2+ Device IDs and the SMETS2+ Device Trust Anchor Cell which is populated with information from the affected Organisation Certificate. In addition, a SMKI ARO acting on behalf of the affected Subscriber shall, as soon as reasonably practicable, submit an Anomaly Detection Thresholds File to the DCC, which shall include amended Anomaly Detection Thresholds that they estimate will be required to resolve the Compromise. The affected Subscriber shall ensure that the Anomaly Detection Thresholds File is: a) submitted using the mechanism specified in the TADP; b) in the format as set out in section 5.3 of the TADP; and c) Digitally Signed using the Private Key	Subscriber	4.2.1.3

		corresponding with a File Signing Certificate issued to the Subscriber for the purpose of Digital Signing of files as set out in section 6 of the TADP.		
4.2.1.3	As soon as reasonably practicable, following 4.2.1.2	The DCC shall notify the SMKI PMA, via a secured electronic means, as soon as reasonably practicable, that a Subscriber wishes the DCC to recover from the Compromise of an Organisation Certificate or Organisation Certificates, using the procedure as set out in section 4.2.2 of this document (which requires use by the DCC of the Recovery Private Key to replace Certificates on SMETS2+ Devices). The DCC shall disable processing of communications destined for SMETS2+ Devices that it has been notified (in Step 4.2.1.2) are affected by the Compromise, for all Parties other than the DCC, by setting the SMI Status of those SMETS2+ Devices to 'recovery'. The DCC shall then request a decision from the SMKI PMA as to whether recovery should be carried out.	DCC	4.2.1.4
4.2.1.4	As soon as reasonably practicable, following 4.2.1.3	The DCC shall take all reasonable steps to provide information to the SMKI PMA to support the SMKI PMA's consideration of what procedural steps (if any) that should be taken in order to recover from the Compromise, where such information may include (but shall not be limited to): a) the number of affected SMETS2+ Devices, which may be provided in in one or more Organisation Compromise Notification Files that comply with Appendix B of this document; b) the extent to which the vulnerabilities that caused the Compromise have been addressed; c) the steps that DCC reasonably believes should be taken to recover from the Compromise; and d) anticipated timescales for recovery. The affected Subscriber shall take reasonable steps to provide information to the DCC in order for the DCC to provide such information to the SMKI PMA.	DCC, Subscriber	4.2.1.5
4.2.1.5	As soon as reasonably practicable, following 4.2.1.4	The DCC shall notify the relevant Network Parties via secured electronic means: a) that a Responsible Supplier wishes to recover using the procedure as set out in section 4.2.2 of this document; and b) the SMETS2+ Device IDs to which the Compromise relates, which shall be submitted in	DCC	4.2.1.6

		one or more Organisation Compromise Notification Files that comply with Appendix B of this document.		

4.2.1.6	As soon as reasonably practicable, following 4.2.1.5	Where the DCC believes that use of the Recovery Private Key is likely to be agreed by the SMKI PMA, the DCC shall identify such preparatory steps that it considers appropriate and either take such steps or instruct Parties to take steps as required, which may include (but shall not be limited to): a) determine the number of Key Custodians required to attend a Key Activation Ceremony for the Recovery Private Key (which may be greater than the minimum number required to activate the Recovery Private Key); b) inform such Key Custodians in respect of the Recovery Private Key, via a secured electronic means, of the date, time and location of a Key Activation Ceremony for the Recovery Private Key; c) notifying Key Custodians to attend the location at which a relevant Key Activation Ceremony may be required; and d) activities required to prepare such systems environments that are required to support activation and use of the Recovery Private Key.	DCC, Key Custodians	4.2.1.7

4.2.1.7	As soon as reasonably practicable, following 4.2.1.6	The SMKI PMA shall: a. determine which of the steps (if any) as set out in section 4.2.2 of this document should be executed, in order to recover from the Compromise; and b. confirm whether the timescales proposed	SMKI PMA, DCC	4.2.1.8

		by the DCC (following consultation with the affected Subscriber(s)) in step 4.2.1.4 for recovery, are approved or whether alternate timescales should apply; and c. if the SMKI PMA has determined that steps in this procedure should be undertaken, detail the timing of actions that the Subscriber is to undertake, in terms of Private Key destruction and Certificate revocations, pursuant to section 4.2.2.10. The SMKI PMA shall inform the DCC of its decision via a secured electronic means.		

4.2.1.8	As soon as reasonably practicable,	The DCC shall inform the affected Subscriber, of the SMKI PMA's decision whether or not to execute the procedure as set out in section 4.2.2,	DCC	If SMKI PMA determines that no

	following 4.2.1.7	and the timing of the section 4.2.2.10 actions that the Subscriber must undertake.		action is required, end of Procedure; otherwise procedure as set out in section 4.2.2 of this document

4.2.2 Execution of Recovery Procedure

The procedure as set out immediately below, amended as instructed by the SMKI PMA, shall be used following execution of the process as set out in section 4.2.1 of this document.

Step	When	Obligation	Responsibility	Next Step
4.2.2.1	As soon as possible, following notification from the SMKI PMA to the DCC that this procedure should be executed	Should the decision of the SMKI PMA be not to disable device communications, the DCC shall re-enable communications to any SMETS2+ Devices where communications have previously been disabled by setting the SMI Status of any SMETS2+ Device that had been set to "recovery" pursuant to Step 4.2.1.3 back to the SMI Status each such SMETS2+ Device held immediately prior to the execution of step 4.2.1.3 of this procedure.	DCC	4.2.2.2
4.2.2.2	As soon as reasonably practicable, following 4.2.2.1	Where: a. The DCC is to issue Commands using the Recovery Private Key, the DCC shall, where necessary, amend the relevant Anomaly Detection Thresholds; and b. the affected	DCC (DSP TAD)	4.1A.2.3

		Subscriber is to submit Service Requests to replace DCC Access Control Broker Certificates with Organisation Certificates, the Subscriber shall submit the necessary revised Anomaly Detection Thresholds in accordance with the TADP. The DCC shall inform, via secured electronic means, a SMKI SRO and the SMKI ARO that provided the details in step 4.2.1.2, that the Anomaly Detection Threshold values have been successfully amended.		
4.2.2.3	As soon as reasonably practicable, following 4.2.2.2	The DCC, in collaboration with Key Custodians, shall participate in a Key Activation Ceremony to activate the Recovery Private Key.	DCC	4.2.2.4

4.2.2.4	As soon as reasonably practicable, following 4.2.2.3	The DCC shall send Commands to each affected SMETS2+ Device, Digitally Signed using the Recovery Private Key, in order to replace Organisation Certificates in all of the Supplier Trust Anchor Cells on SMETS2+ Devices as notified in step 4.2.1.2, with a DCC Access Control Broker Certificate. In doing so, the DCC shall monitor its Command acknowledgement records, to determine the progress of recovery in respect of SMETS2+ Devices affected by the Compromise.	DCC	4.2.2.5
4.2.2.5	As soon as reasonably practicable, following 4.2.2.4	Upon completion of step 4.2.2.4 for each SMETS2+ Device, the DCC shall restore processing of communications destined for the affected SMETS2+ Device by setting the SMI Status to ‘recovered’.	DCC	4.2.2.6
4.2.2.6	As soon as reasonably practicable, following 4.2.2.5	The DCC shall notify the affected Subscriber of the replacement of Organisation Certificates on affected SMETS2+ Devices: a. upon replacement of affected Organisation Certificates on each SMETS2+ Device, using a DCC Alert issued via the DCC User Interface; and b. upon completion of attempts to replace all affected Organisation Certificates on relevant SMETS2+ Devices, in one or more Organisation Compromise Recovery Progress Files that comply with Appendix C of this document, provided via secured electronic means.	DCC	4.2.2.7
4.2.2.7	As soon as reasonably practicable, following 4.2.2.6	The affected Subscriber shall either: a. identify replacement Organisation Certificates; or b. submit such Certificate Signing Requests (CSRs) that are required in order to acquire new Organisation Certificates.	Subscriber	4.2.2.8
4.2.2.8	As soon as reasonably practicable, following 4.2.2.7	Where the DCC has recovered by replacing Organisation Certificates of the Responsible Supplier, with a DCC Access Control Broker Certificate, the Responsible Supplier shall submit Service Requests, in accordance with the provisions of the DCC User Interface Specification, to replace the DCC Access Control Broker Certificate in each Supplier SMETS2+ Device slot with a replacement Organisation Certificate, for	Responsible Supplier	4.2.2.9

		each SMETS2+ Device as established in step 4.2.1.1 within section 4.2 of this document. Upon successful completion of such replacement for a SMETS2+ Device, the DCC shall set the SMI Status for that SMETS2+ Device to the SMI Status that was in place immediately prior to the execution of step 4.2.2.1 of this procedure.		
4.2.2.9	As soon as reasonably practicable, following 4.2.2.8	The Responsible Supplier shall notify the DCC in respect of replacement of such DCC Access Control Broker Certificates with new Organisation Certificates, via secured electronic means and in one or more Organisation Compromise Recovery Progress Files that comply with Appendix C of this document.	DCC	Procedure as set out in Section 4.2.2.10 of this document.
4.2.2.10	As required by the SMKI PMA	Where required by the SMKI PMA, the affected Subscriber shall submit Certificate Revocation Requests (CRRs), as set out in the SMKI RAPP, in order to revoke affected Organisation Certificates. The DCC shall revoke Organisation Certificates in accordance with the provisions of the Appendix B of the Code and the SMKI RAPP. Where required by the SMKI PMA, the affected Subscriber shall destroy the Private Key associated with the revoked Organisation Certificate.	Subscriber, DCC	Procedure as set out in section 4.2.3 of this document

4.2.3 Post-Recovery

The procedure as set out immediately below shall be used following execution of the procedures as set out in sections 4.2.1 and 4.2.2 of this document.

Step	When	Obligation	Responsibility	Next Step
4.2.3.1	As soon as reasonably practicable, following completion of the procedure as set out in Section 4.2.2 of this document	A SMKI ARO acting on behalf of the affected Subscriber shall, as soon as reasonably practicable, submit appropriate enduring Anomaly Detection Thresholds to the DCC in accordance with the TADP. The DCC shall amend the relevant Anomaly Detection Thresholds to the values as submitted by the affected Subscriber, including performing the checks and validations set out in the TADP. The DCC shall reinstate its relevant Anomaly Detection Threshold values that were in place immediately prior to the temporary values used	DCC (DSP TAD)	4.2.3.2

		during the execution of the procedure set out in this Section 4.2 of this document.		

4.2.3.2	As soon as reasonably practicable, following 4.2.3.1	The DCC shall notify the SMKI PMA, via a secured means, of: a. whether the recovery from the Compromise has been successfully completed, which may be provided in one or more Organisation Compromise Recovery Progress Files that comply with Appendix C of this document; and b. the number of SMETS2+ Devices for which recovery was not successful.	DCC	End of procedure

4.3. Method 3 - recovery by the DCC using the Recovery Private Key to place new Organisation Certificates on SMETS2+ Devices

4.3.1 Pre-Recovery

The DCC shall execute the procedure as set out immediately below, following notification of the Compromise of the Private Key associated with the Public Key contained within an Organisation Certificate, in accordance with section 3.2 of this document, and notification from the relevant Subscriber that it wishes to recover from the Compromise using the procedure set out in this section.

The affected Subscriber shall only request use of the procedure in this section having considered the Recovery Action Risks, including that section 4.3.1.3 requires the DCC to disable access, via the DCC, to affected Devices **before the SMKI PMA has reached a decision as to whether to proceed**. For clarity, this includes all prepayment functionality operated via the DCC.

Step	When	Obligation	Responsibility	Next Step
4.3.1.1	As soon as possible, following notification that the Subscriber wishes to recover using the procedure set out in section 4.3.2 of this document	The affected Subscriber should not take any action, prior to the SMKI PMA making a decision as to whether to use this procedure, that would prejudge that outcome unless they consider risks are sufficient to justify such advance actions. For clarity, this includes the actions to which Recovery Action Risks relate.	Subscriber, DCC	4.3.1.2
4.3.1.2	As soon as reasonably practicable, following 4.3.1.1	A SMKI ARO acting on behalf of the affected Subscriber shall submit to the DCC, via secured electronic means, one or more files which shall be Organisation Compromise Notification Files as set out in Appendix B for Subscribers that are not the	Subscriber	4.3.1.3

		DCC, or Other Compromise Notification Files as set out in Appendix D where the Subscriber is the DCC. The affected Subscriber should ensure that such files together contain details of: a. the Incident to which the submission relates; b. the EUI-64 identifiers for the organisation that is the affected Subscriber to which the Compromise, or suspected Compromise relates; and c. for each Organisation Certificate that is affected by the Compromise, the serial number of the Organisation Certificate, the SMETS2+ Device IDs and the SMETS2+ Device Trust Anchor Cell which is populated with information from the affected Organisation Certificate.		

4.3.1.3	As soon as reasonably practicable, following 4.3.1.2	The DCC shall notify the SMKI PMA, via a secured electronic means, as soon as reasonably practicable, that a Subscriber wishes the DCC to recover from the Compromise of its Organisation Certificate using the procedure as set out in section 4.3.2 of this document (which requires use by the DCC of the Recovery Private Key to replace Organisation Certificates on SMETS2+ Devices). Where the Compromise affects Certificates where the Remote Party Role is supplier or wanProvider (with their GBCS meaning) the DCC shall disable processing of communications destined for those SMETS2+ Devices that it has been notified (in Step 4.3.1.2) that are affected by the Compromise, for all Parties other than the DCC, by setting the SMI Status of those SMETS2+ Devices to 'recovery'. The DCC shall request a decision from the SMKI PMA as to whether recovery should be carried out.	DCC	4.3.1.4

4.3.1.4	As soon as reasonably practicable, following 4.3.1.3	Where the affected Subscriber is not the Responsible Supplier for a SMETS2+ Device that is notified in step 4.3.1.2, the DCC shall notify the Responsible Supplier via secured electronic means: a. that a Subscriber wishes to recover using the procedure as set out in section 4.3.2 of this document; and b. the SMETS2+ Device IDs to which the Compromise relates, which shall be submitted in one or more one or more files which shall be Organisation Compromise Notification Files as set out	DCC	4.3.1.5

		in Appendix B for Subscribers that are not the DCC, or Other Compromise Notification Files as set out in Appendix D where the Subscriber is the DCC.		
4.3.1.5	As soon as reasonably practicable, following 4.3.1.4	The DCC shall take all reasonable steps to provide information to the SMKI PMA to support the SMKI PMA's consideration of what procedural steps (if any) that should be taken in order to recover from the Compromise, where such information may include (but shall not be limited to): a. the number of affected SMETS2+ Devices, which may be provided in one or more one or more files which shall be Organisation Compromise Notification Files as set out in Appendix B for Subscribers that are not the DCC, or Other Compromise Notification Files as set out in Appendix D where the Subscriber is the DCC; b. the extent to which the vulnerabilities that caused the Compromise have been addressed; c. the steps that DCC reasonably believes should be taken to recover from the Compromise; and d. anticipated timescales for recovery. The affected Subscriber shall take reasonable steps to provide information to the DCC in order for the DCC to provide such information to the SMKI PMA.	DCC, Subscriber	4.3.1.6
4.3.1.6	As soon as reasonably practicable, following 4.3.1.5	Where the DCC believes that use of the Recovery Private Key is likely to be required by the SMKI PMA, the DCC shall identify such preparatory steps that it considers appropriate and either take such steps or instruct Parties to take steps as required, which may include (but shall not be limited to): a. determine the number of Key Custodians required to attend a Key Activation Ceremony for the Recovery Private Key (which may be greater than the minimum number required to activate the Recovery Private Key); b. inform such Key Custodians in respect of the Recovery Private Key, via a secured electronic means, of the date, time and location of a Key Activation Ceremony for the Recovery Private Key; c. notifying Key Custodians to attend the	DCC, Key Custodians	4.3.1.7

		location at which a relevant Key Generation Ceremony or Key Activation Ceremony may be required; and d. activities required to prepare such systems environments that are required to support activation and use of the Recovery Private Key.		

4.3.1.7	As soon as reasonably practicable, following 4.3.1.6	The SMKI PMA shall: a. determine which of the steps (if any) as set out in section 4.2.2 of this document should be executed, in order to recover from the Compromise; b. confirm whether the timescales proposed by the DCC (following consultation with the affected Subscriber(s)) in step 4.3.1.5 for recovery, are approved or whether alternate timescales should apply; and c. if the SMKI PMA has determined that steps in this procedure should be undertaken, detail the actions that the Subscriber is to undertake, in	SMKI PMA, DCC	4.3.1.8

		terms of Private Key Destruction and Certificate revocations, including their timing. The SMKI PMA shall inform the DCC of its decision via a secured electronic means.		
4.3.1.8	As soon as reasonably practicable, following 4.3.1.7	The DCC shall notify the affected Subscriber, via secured electronic means, of the SMKI PMA's decision whether or not to execute the procedure (amended as directed by the SMKI PMA) as set out in section 4.3.2 and of the action the SMKI PMA requires the Subscriber to take in terms of Private Key destruction and Certificate revocation, and their timing. Where the affected Subscriber is not the Responsible Supplier for a SMETS2+ Device that is notified in step 4.3.1.2, the DCC shall notify the Responsible Supplier via secured electronic means, of the SMKI PMA's decision whether or not to execute the procedure (amended as directed by the SMKI PMA) as set out in section 4.3.2.	DCC	If SMKI PMA determines that no action is required, end of Procedure; otherwise procedure as set out in section 4.3.2 of this document

4.3.2 Execution of Recovery Procedure

The procedure as set out immediately below, amended as instructed by the SMKI PMA in accordance with section 4.3.1 of this document, shall be used, following execution of the process as set out in section 4.3.1 of this document.

Step	When	Obligation	Responsibility	Next Step
4.3.2.1	As soon as possible, following notification from the SMKI PMA to the DCC that this procedure should be executed	Should the decision of the SMKI PMA be not to disable device communications, the DCC shall re-enable communications to any devices where communications have previously been disabled by setting the SMI Status of any SMETS2+ Device that had been set to "recovery" pursuant to Step 4.3.1.3 back to the SMI Status each such SMETS2+ Device held immediately prior to the execution of step 4.3.1.3 of this procedure.	DCC	4.3.2.2

4.3.2.2	As soon as possible, following 4.3.2.1	Where necessary, the DCC shall temporarily amend the relevant Anomaly Detection Thresholds, for: a) the DCC that relate to the issuance of Commands to replace Organisation Certificates on SMETS2+ Devices, to enable replacement of affected Organisation Certificates as notified in section 4.3.1 of this document. The DCC shall inform, via secured electronic means, a SMKI SRO and the SMKI ARO that provided the details in step 4.3.1.2, that the Anomaly Detection Threshold values have been successfully amended.	DCC (DSP TAD)	4.3.2.3
4.3.2.3	As soon as reasonably practicable, following 4.3.2.2	The affected Subscriber shall either: a. identify replacement Organisation Certificates that are not Digitally Signed by the Compromised Private Key; or b. submit such Certificate Signing Requests (CSRs) that are required in order to acquire new Organisation Certificates that are not Digitally Signed by the Compromised Private Key. The affected Subscriber shall notify the DCC of the serial numbers of the replacement Organisation Certificates that should be used to populate a SMETS2+ Device and specify the SMETS2+ Device Trust Anchor Cell to which the replacement Organisation Certificate relates, which shall be provided via secured electronic means in one or more one or more files which shall be Organisation Compromise Notification Files as set out in Appendix B for Subscribers that are not the DCC, or Other Compromise Notification Files as set out in Appendix D where the Subscriber is the DCC.	Subscriber	4.3.2.4
4.3.2.4	As soon as reasonably practicable, following 4.3.2.3	The DCC, in collaboration with Key Custodians, shall participate in a Key Activation Ceremony to activate the Recovery Private Key.	DCC	4.3.2.5
4.3.2.5	As soon as reasonably practicable, following 4.3.2.4	The DCC shall send Commands to all SMETS2+ Devices, Digitally Signed using the Recovery Private Key, in order to replace affected Organisation Certificates on relevant SMETS2+ Devices as notified in step 4.3.1.1 with replacement Organisation Certificates as notified by the affected Subscriber. In doing so, the DCC	DCC	4.3.2.6

		shall monitor its Command acknowledgement records, to determine the progress of recovery in respect of SMETS2+ Devices affected by the Compromise.		
4.3.2.6	As soon as reasonably practicable, following 4.3.2.5	The DCC shall notify the affected Subscriber of the replacement of Organisation Certificates on affected SMETS2+ Devices: a. upon replacement of affected Organisation Certificates on each SMETS2+ Device, using a DCC Alert issued via the DCC User Interface; and b. upon completion of attempts to replace all affected Organisation Certificates on relevant SMETS2+ Devices, in one or more files which shall be Organisation Compromise Recovery Progress Files as set out in Appendix C for Subscribers that are not the DCC, or Other Compromise Recovery Progress Files as set out in Appendix E where the Subscriber is the DCC, provided by secured electronic means.	DCC	4.3.2.7
4.3.2.7	As soon as reasonably practicable, following 4.3.2.6	Upon completion of step 4.3.2.6 for each SMETS2+ Device, the DCC shall restore processing of communications destined for the affected SMETS2+ Device by setting the SMI Status for that SMETS2+ Device to the SMI Status that was in place immediately prior to the execution of step 4.3.2.1 of this procedure.	DCC	4.3.2.8
4.3.2.8	As soon as reasonably practicable, following 4.3.2.7	The DCC shall notify each Responsible Supplier for affected SMETS2+ Devices, by secured electronic means, which SMETS2+ Devices were not recovered successfully in one or more one or more files which shall be Organisation Compromise Recovery Progress Files as set out in Appendix C for Subscribers that are not the DCC, or Other Compromise Recovery Progress Files as set out in Appendix E where the Subscriber is the DCC.	DCC	Procedure as set out in Section 4.3.3 of this document.

4.3.3 Post-Recovery

The procedure as set out immediately below shall be used following execution of the procedures as set out in sections 4.3.1 and 4.3.2 of this document.

Step	When	Obligation	Responsibility	Next Step

4.3.3.1	As soon as reasonably practicable, following completion of the procedure as set out in Section 4.3.2 of this document	The DCC shall reinstate its relevant Anomaly Detection Threshold values that were in place immediately prior to the temporary values used during the execution of the procedure set out in this Section 4.3 of this document.	DCC (DSP TAD)	4.3.3.2
4.3.3.2	As soon as reasonably practicable, following 4.3.3.1	The DCC shall notify the SMKI PMA, via a secured electronic means, of: a. whether the recovery from the Compromise has been successfully completed, which may be provided in one or more files which shall be Organisation Compromise Recovery Progress Files as set out in Appendix C for Subscribers that are not the DCC, or Other Compromise Recovery Progress Files as set out in Appendix E where the Subscriber is the DCC; and b. the number of SMETS2+ Devices for which recovery was not successful.	DCC	End of procedure

5. Recovery using the Contingency Private Key

5.1 Pre-Recovery

The DCC shall execute the procedure as set out immediately below, following:

a) the notification of the Compromise of the Root OCA Private Key, in accordance with section 3.2 of this document; or

b) where the use of the Recovery Private Key has been unsuccessful (as set out in sections 4.2, 4.3, 6.2 and 6.3 of this document) and the DCC reasonably believes that the nature of the Compromise could require use of the Contingency Private Key.

The DCC shall only request use of the procedure in this section having considered the Recovery Action Risks, including that, for the time between the action in section 5.2.1 and those in section 5.3.2, access, via the DCC, to affected Devices will not be possible. For clarity, this includes all prepayment functionality operated via the DCC.

Step	When	Obligation	Responsibility	Next Step
5.1.1	As soon as reasonably practicable, following	The DCC shall notify the SMKI PMA and all affected Subscribers, via a secured electronic means, as soon as reasonably practicable, that a Compromise of the Root OCA Key has been	DCC	5.1.2

	notification of the Compromise of the Root OCA Private Key or escalation due to failure of recovery using the Recovery Private Key, in accordance with section 3.2 of this document	notified, or that use of the Recovery Private Key has been unsuccessful that the DCC reasonably believes that the nature of the Compromise could require use of the Contingency Private Key. The DCC shall also provide details to affected Subscribers of the affected SMETS2+ Devices and Organisation Certificates, in one or more Other Compromise Notification files which comply with Appendix D of this document. The DCC shall request a decision from the SMKI PMA as to whether recovery should be carried out.		
5.1.2	As soon as reasonably practicable, following 5.1.1	The DCC shall take all reasonable steps to provide information to the SMKI PMA to support the SMKI PMA's consideration of what procedural steps (if any) that should be taken in order to recover from the Compromise, where such information may include (but shall not be limited to): a. the affected SMETS2+ Devices and Subscribers, which may be provided in one or more Other Compromise Notification files which comply with Appendix D of this document; b. the extent to which DCC's monitoring indicates that there has been unauthorised use of the Root OCA Private Key; c. the extent to which the vulnerabilities that caused the Compromise have been addressed; d. information relevant to the SMKI PMA's consideration of the Recovery Action Risks; e. the steps that DCC reasonably believes should be taken to recover from the Compromise; and f. anticipated timescales for recovery.	DCC	5.1.3
5.1.3	As soon as reasonably practicable, following 5.1.2	Where the DCC believes that use of the Contingency Private Key is likely to be required by the SMKI PMA, it shall identify such preparatory steps that it considers appropriate and to either take such steps or instruct Parties to take steps as required, including (but not limited to): a. inform the requisite number of Key Custodians, via a secured electronic	DCC, Key Custodians	5.1.4

		means, that a Key Activation Ceremony for the Contingency Private Key is required (which may be greater than the minimum number required to activate the Contingency Private Key), and the date, time and location of each Key Activation Ceremony; b. notifying Key Custodians to attend the location at which a relevant Key Activation Ceremony may be required; and c. activities required to prepare the systems environment required to support activation and use of the Contingency Private Key.		
5.1.4	As soon as reasonably practicable, following 5.1.3	Having considered the Recovery Action Risks, the SMKI PMA shall: a. determine which of the steps (if any) as set out in section 4.2.2 of this document should be executed, in order to recover from the Compromise; b. confirm whether the timescales proposed by the DCC (following consultation with the affected Subscriber(s)) in step 5.1.2 for recovery, are	SMKI PMA, DCC	If SMKI PMA determines that no action is required, end of Procedure; otherwise 5.1.5

		approved or whether alternate timescales should apply; and c. for Certificates and Private Keys in the scope of section 5.1.6, determine which of the DCC controlled Private Keys are to be destroyed, and which of the DCC controlled Certificates are to be revoked and when. For clarity, the old Contingency Symmetric Key and old Contingency Private must not be destroyed until all Commands that are needed pursuant to section 5.2.8 (including for any		

		Device in the supply chain) have been created, since when they are destroyed, no further such Commands can be created. The SMKI PMA shall inform the DCC of its decision via a secured electronic means.		
5.1.5	As soon as reasonably practicable, following 5.1.4	The DCC shall notify affected Subscribers, via a secured electronic means, of the SMKI PMA's decision whether or not to execute the recovery procedure (amended as directed by the SMKI PMA) as set out in section 5.2.	DCC	Where required by SMKI PMA, 5.1.6; otherwise End of procedure
5.1.6	As directed by the SMKI PMA	The DCC shall execute steps in order, where applicable in accordance with the SMKI PMA's decision, to revoke: a. the Root OCA Certificate; b. the associated Issuing OCA Certificate(s) As described in section 5.1.4c, the DCC may be directed to update and lodge the relevant ARL in the SMKI Repository.	DCC	Procedure as set out in section 5.2 of this document

5.2 Execution of Recovery Procedure

The DCC shall execute the steps as notified by the SMKI PMA, in accordance with the procedure in section 5.1 of this document, which may include (but will not be limited to) some or all of the steps as set out in this section 5.2.

Step	When	Obligation	Responsibility	Next Step
5.2.1	As soon as reasonably practicable, following confirmation of Compromise and instruction from the SMKI PMA that recovery using the Contingency Private Key should be carried out	The DCC shall disable processing of communications destined for SMETS2+ Devices that are affected by the Compromise, for all Parties other than the DCC, by setting the SMI Status to 'recovery'.	DCC	5.2.2
5.2.2	As soon as possible, following 5.2.1	Where: a. The DCC is to issue Commands using the Contingency Private Key, the DCC shall, where necessary, amend the relevant Anomaly Detection Thresholds; and b. the affected Subscriber is to submit Service Requests to replace DCC Access Control	DCC (DSP TAD)	5.2.3

		Broker Certificates with Organisation Certificates, the Subscriber shall submit submit the necessary revised Anomaly Detection Thresholds in accordance with the TADP. The DCC shall inform, via secured electronic means, a SMKI SRO and the SMKI ARO that provided the details in step 5.2.2, that the Anomaly Detection Threshold values have been successfully amended.		
5.2.3	As soon as reasonably practicable, following 5.2.2	The DCC, shall conduct relevant Key Generation Ceremonies in accordance with the Organisation Certificate Policy and Organisation CPS and DCC local procedures, in order to generate: a. a new Root OCA Key Pair; and b. a new Issuing OCA Key Pair.	DCC	5.2.3a
5.2.3a	As soon as reasonably practicable, following 5.2.3	Where directed by the SMKI PMA, the DCC shall conduct relevant Key Generation Ceremonies in accordance with the	DCC (as DSP)	5.2.3b

		Organisation Certificate Policy and Organisation CPS, in order to generate a new Contingency Key Pair. The DCC shall make the public key available to the TSP.		
5.2.3b	As soon as reasonably practicable, following 5.2.3a	Where directed by the SMKI PMA, the DCC shall conduct relevant Key Generation Ceremonies in accordance with the Organisation Certificate Policy and Organisation CPS, in order to generate a new Contingency Symmetric Key. The DCC shall use the new Contingency Symmetric Key to encrypt the new Contingency Public Key to produce the value to be placed in the WrappedApexContingencyKey extension (with the meaning of IETF RFC 5934 section 9) in the new Root OCA Certificate.	DCC (as TSP)	5.2.4
5.2.4	As soon as reasonably practicable, following 5.2.3b	The DCC shall generate a new Root OCA Certificate, embedding the new wrappedApexContingencyKey that has been generated as part of the process as set out in step 5.2.4 of this document. The new Root OCA Certificate shall be Digitally	DCC (as TSP)	5.2.5

		Signed by the new Root OCA Private Key. The DCC shall generate a replacement Issuing OCA Certificate, signed by the new Root OCA Private Key.		
5.2.5	As soon as reasonably practicable, following 5.2.4	The DCC shall lodge the new Root OCA Certificate and Issuing OCA Certificate in the SMKI Repository.	DCC	5.2.6
5.2.6	As soon as reasonably practicable, following 5.2.5	The DCC, in collaboration with Key Custodians, shall participate in a Key Activation Ceremony to activate the old Contingency Private Key and the plain text version of the old Contingency Symmetric Key that were used to generate the wrappedApexContingencyKey that is stored within the old Root OCA Certificate that has been deployed to SMETS2+ Devices. To facilitate this, the DCC shall bring together all parts of the old Contingency Symmetric Key.	DCC (as DSP)	5.2.7
5.2.7	As soon as reasonably practicable, following 5.2.6	The DCC shall send Commands to all SMETS2+ Devices, Digitally Signed using the old Contingency Private Key and including the old Contingency Symmetric Key to	DCC	5.2.8

		enable activation, attaching the following Certificates (where applicable according to the SMETS2+ Device type) to the corresponding SMETS2+ Devices:
		a. a new Root OCA Certificate;
		b. a replacement new DCC Transitional CoS Certificate;
		c. a replacement new Recovery Certificate;
		d. a replacement new DCC Access Control Broker Certificate;
		e. a replacement new DCC WAN Provider Certificate; and
		f. a new DCC Access Control Broker Certificate which shall be placed in each Supplier SMETS2+ Device Trust Anchor Cell or Network Operator SMETS2+ Device Trust Anchor Cell in the corresponding SMETS2+ Device.		

5.2.8	As soon as reasonably practicable, following 5.2.7	Upon completion of step 5.2.7 for each SMETS2+ Device, the DCC shall restore processing of communications destined for the affected SMETS2+ Device by setting the SMI Status to 'recovered'.	DCC	5.2.9
5.2.9	As soon as reasonably practicable, following 5.2.8	The DCC shall monitor its Command acknowledgement records, to determine the progress of recovery in respect of SMETS2+ Devices affected by the Compromise.	DCC	5.2.10
5.2.10	As soon as reasonably practicable, following 5.2.9	The DCC shall notify the affected Subscriber of the replacement of Organisation Certificates on affected SMETS2+ Devices: a. upon replacement of affected Organisation Certificates on each SMETS2+ Device with a DCC Access Broker Certificate, via DCC Alert issued via the DCC User Interface to the affected Subscriber; and b. upon	DCC	5.2.11

		completion of attempts to replace all affected Organisation Certificates (for each affected Subscriber) on relevant SMETS2+ Devices, in one or more Other Compromise Recovery Progress Files that comply with Appendix E of this document, which shall be provided via secured electronic means.		
5.2.11	As soon as reasonably practicable, following 5.2.10	The DCC shall notify each Responsible Supplier for affected SMETS2+ Devices, via secured electronic means, in one or more Other Compromise Recovery Progress Files that comply with Appendix E of this document, which SMETS2+ Devices were not recovered successfully.	DCC	Procedure as set out in Section 5.3 of this document

5.3 Post Recovery

The procedure as set out immediately below shall be used following recovery from the Compromise of a Root OCA Private Key.

Step	When	Obligation	Responsibility	Next Step

5.3.1	As soon as reasonably practicable, following completion of the procedure as set out in Section 5.2 of this document	The affected Subscriber shall generate new Private Keys and Certificate Signing Requests (CSRs), and submit such CSRs that are required in order to acquire new associated Organisation Certificates.	Subscriber	5.3.2

5.3.2	As soon as reasonably practicable, following 5.3.1	The Responsible Supplier shall submit Service Requests, in accordance with the provisions of the DCC User Interface Specification, to replace: a. the DCC Access Control Broker Certificate in each Supplier SMETS2+ Device Trust Anchor Cell with a replacement Organisation Certificate that is Issued under the new Issuing OCA, for each SMETS2+ Device as established in step 5.2.2 within section 5.2 of this document; and b. the DCC Access Control Broker Certificate in each Network	Subscriber	5.3.3

		Operator SMETS2+ Device Trust Anchor Cell with an Organisation Certificate to which the Network Operator is the Subscriber that is Issued under the new Issuing OCA, for each SMETS2+ Device as established in step 5.2.2 within section 5.2 of this document. Upon successful completion of such replacement for a SMETS2+ Device, the DCC shall set the SMI Status for that SMETS2+ Device to the SMI Status that was in place immediately prior to the execution of step 5.2.1 of this procedure. The Responsible Supplier shall notify the DCC in respect of replacement of affected Organisation Certificates, via secured electronic means and in one or more Other Compromise Recovery Progress Files that comply with Appendix E of this document.		

5.3.3	As soon as reasonably practicable, following 5.3.2	A SMKI ARO acting on behalf of each affected Subscriber shall, as soon as reasonably practicable, submit appropriate enduring Anomaly Detection Thresholds to the DCC, which shall be submitted as a file as set out in section 5.1 of the TADP that is Digitally Signed using the Private Key corresponding with a File Signing Certificate issued to the Subscriber for the purpose of Digital Signing of files. The DCC shall amend the relevant Anomaly Detection Thresholds to the values as submitted by the affected Subscriber, including performing the checks and validations set out in the TADP. The DCC shall reinstate its relevant Anomaly Detection Threshold values that were in place immediately prior to the temporary values used during the execution of the procedure set out in this Section 5 of this document.	Subscriber, DCC (DSP TAD)	5.3.4

5.3.4	As soon as reasonably practicable, following 5.3.3	The DCC shall notify the SMKI PMA and affected Subscribers, via a secured means, of: a. whether the recovery from the Compromise has been successfully completed, which may be provided in one or more Other Compromise Recovery Progress Files that comply with Appendix E of this document.; and b. the number of	DCC	5.3.5

		SMETS2+ Devices for which recovery was not successful.		

5.3.5	As soon as reasonably practicable, following 5.3.4	If the compromised key material remains available to the DCC, then the DCC may be directed by the SMKI PMA to issue CRLs/ARLs for the impacted Organisation Certificates. The DCC may also be directed by the SMKI PMA to revoke and destroy affected Private Keys and Symmetric Keys, which may include: a. the old Root OCA Private Key; b. the old Issuing OCA Private Key(s); c. the old Contingency Private Key; and/or d. the old Contingency Symmetric Key.	DCC	End of procedure

6. Recovery from Compromise of a Contingency Private Key, Contingency Symmetric Key, Recovery Private Key or Issuing OCA Private Key

6.1 Recovery from Compromise of a Contingency Private Key or the Contingency Symmetric Key

This will replace only the Root OCA Certificate. All subordinate Certificates remain valid as the Root OCA Key Pair does not change.

6.1.1 Pre-Recovery

Where the DCC becomes aware that a Compromise to the Contingency Private Key or the Contingency Symmetric Key has occurred, the DCC shall raise an Incident in accordance with sections 2.1 and 2.2 of the Incident Management Policy and shall execute the procedure as set out immediately below.

Step	When	Obligation	Responsibility	Next Step
6.1.1.1	As soon as reasonably practicable, following notification of the Compromise of the Contingency Private Key or Contingency Symmetric Key, in accordance with section 3.2 of this document	The DCC shall notify the SMKI PMA, via a secured electronic means, as soon as reasonably practicable, that a Compromise, or suspected Compromise, of the Contingency Private Key or Contingency Symmetric Key has been notified. The DCC shall request a decision from the SMKI PMA as to whether recovery should be carried out.	DCC	6.1.1.2
6.1.1.2	As soon as reasonably practicable, following 6.1.1.1	The DCC shall take all reasonable steps to provide information to the SMKI PMA to support the SMKI PMA's consideration of what procedural steps (if any) that should be taken in order to recover from the Compromise, where such information may include (but shall not be limited to): a. the extent to which the vulnerabilities that caused the Compromise have been addressed; b. the extent to which DCC's monitoring indicates that there has been	DCC, SMKI PMA	6.1.1.3

		unauthorised use of the Contingency Private Key and/or Contingency Symmetric Key; c. the likely impact on Services if Recovery is carried out; d. the likely impact on Services if the Compromise were to be exploited; e. the steps that DCC reasonably believes should be taken to recover from the Compromise; and f. anticipated timescales for recovery.		

6.1.1.3	As soon as reasonably practicable, following 6.1.1.2	Where the DCC believes that replacement of the Contingency Key Pair and generation of a replacement Root OCA Certificate (and therefore a new Contingency Private Key and Contingency Symmetric Key) is likely to be required by the SMKI PMA, it shall identify such preparatory steps that it considers appropriate and to take steps as required, including (but not limited to): a. informing the requisite number of Key Custodians, via a secured electronic means, that a Key Generation Ceremony for the Contingency Key Pair, and for the Contingency Symmetric Key is required and the date, time and location of each such Key Generation Ceremony; b. notifying Key Custodians to attend the	DCC, Key Custodians	6.1.1.4

		relevant Key Generation Ceremony; and c. activities required to prepare such systems environment required to support: a. generation of a new Contingency Key Pair; b. creating a new M#N Share of the Contingency Private Key; c. generation of a new Contingency Symmetric Key; d. encryption of the new Contingency Public Key using the new Contingency Symmetric Key; e. for the new symmetric key, conducting Contingency Symmetric Key Splitting; f. generation of a replacement Root OCA Certificate, containing the Public Key from the current Root OCA Certificate and the new encrypted Contingency Public Key.		

6.1.1.4	As soon as reasonably practicable, following 6.1.1.3	The SMKI PMA shall: a. determine which of the steps (if any) as set out in section 5 4.2.2 of this document should be executed, in order to recover from the Compromise; b. confirm whether the timescales proposed by the DCC in step 6.1.1.3 for recovery, are approved or whether alternate timescales should apply; and c. consider preparing a communication for notifying Subscribers and instruct the DCC that the SMKI PMA will determine whether and, if so, what the timing of issue should be of any such a notification. The SMKI PMA shall inform the DCC of its decision via a secured electronic means.	SMKI PMA, DCC	If SMKI PMA determines that no action is required, end of procedure; otherwise 6.1.2

6.1.2 Execution of Recovery Procedure

The procedure as set out immediately below, amended as instructed by the SMKI PMA, shall be used following execution of the process as set out in section 6.1.1 of this document.

Step	When	Obligation	Responsibility	Next Step
6.1.2.1	As soon as reasonably practicable, following confirmation of Compromise and instruction from the SMKI PMA that this recovery procedure should be carried out	The DCC shall temporarily amend the Anomaly Detection Thresholds for the CS02b Update Security Credentials (anyExceptAbnormalRootByRecovery) Command (where those terms have their GBCS meaning) from 0 to the level required to instruct all affected SMETS2+ Devices. The DCC should perform the checks and validations set out in the TADP, for the DCC that relate to the issuance of recovery Commands to replace Root OCA Certificates on SMETS2+ Devices.	DCC	6.1.2.2
6.1.2.2	As soon as reasonably practicable, following 6.1.2.1	Where directed by the SMKI PMA, the DCC shall conduct relevant Key Generation Ceremonies in accordance with the Organisation Certificate Policy and Organisation CPS, in order to generate a new Contingency Key Pair. The DCC shall securely transport the new Contingency Public Key from DSP to TSP.	DCC (as DSP)	6.1.2.2a
6.1.2.2a	As soon as reasonably practicable, following 6.1.2.2	Where directed by the SMKI PMA, in accordance with 6.1.2.2, the DCC shall conduct relevant Key Generation Ceremonies in accordance with the Organisation Certificate Policy and Organisation CPS, in order to generate a new Contingency Symmetric Key. The DCC shall use the new Contingency Symmetric Key to encrypt the new Contingency Public Key to produce the value to be placed in the `WrappedApexContingencyKey` extension (with the meaning of IETF RFC 5934 section 9) in the new Root OCA Certificate.	DCC (as TSP)	6.1.2.3
6.1.2.3	As soon as reasonably practicable, following 6.1.2.2	The DCC shall generate a new Root OCA Certificate, embedding the new `WrappedApexContin`	DCC (as TSP)	6.1.2.4

		gencyKey that has been generated as part of the process as set out in step 6.1.2.2 of this document. The replacement Root OCA Certificate shall be Digitally Signed by the existing Root OCA Private Key.		
6.1.2.4	As soon as reasonably practicable, following 6.1.2.4	The DCC shall lodge the new Root OCA Certificate in the SMKI Repository.	DCC	6.1.2.5
6.1.2.5	As soon as reasonably practicable, following 6.1.2.4	The DCC shall: a. retrieve only the new Root OCA Certificate from the SMKI Repository; b. create the CS02b Update Security Credentials (anyExceptAbnormalRootByRecovery) Commands (where those terms have their GBCS meaning) as are required to replace the existing Root OCA Certificate alone on all SMETS2+ Devices (excluding IHDs) with the new Root OCA Certificate. c. In such Commands the DCC shall use the new Root OCA Certificate as both the NewWithOld and NewWithNew certificates (where those terms have their GBCS meaning); and d. Shall produce a list of the affected Devices by type in a proposed priority order of ESME, SAPC, HCALCS, GSME and PPMID and provide this to the SMKI PMA seeking guidance on any other prioritisation that might be needed.	DCC	6.1.2.6
6.1.2.6		On receipt of guidance from the SMKI PMA on any other priority order for recovery, the DCC shall send the resulting Commands to the target SMETS2+ Devices, undertaking retries where Responses indicate failure or Responses are not received.	DCC	6.1.2.7
6.1.2.7	As soon as reasonably	The DCC shall monitor Responses to the Commands sent pursuant to 6.1.2.5, to determine the progress of recovery in respect of replacement of the Root OCA Certificate on SMETS2+ Devices.	DCC	6.1.2.8

	practicable, following 6.1.2.6	The DCC shall also continue to monitor for any unauthorised use of the Contingency Private Key/Contingency Symmetric Key and shall take all reasonable steps to keep the SMKI PMA informed of progress throughout and of any such unauthorised use. Where directed by the SMKI PMA to amend the recovery steps as a result of unauthorised use, the DCC execute steps as notified by the SMKI PMA.		
6.1.2.8	As soon as reasonably practicable, following 6.1.2.6	The DCC shall update the SMKI PMA with regular progress reports throughout the Recovery process on the steps taken; on the volumes of SMETS2+ Devices that are satisfactorily updated; on the volumes remaining to be updated; and on the number, type and Responsible Supplier of failed retries and shall seek a direction on: a. when to stop further re-tries; b. if and when to notify Subscribers; and c. for details of any communication to be sent to Subscribers.	DCC	6.1.3
6.1.2.9	As soon as reasonably practicable, following 6.1.2.8	On receipt of notification from the SMKI PMA, the DCC shall follow the instruction to either: a. continue to make efforts to recover all or some of the affected SMETS2+ Devices; or b. cease the recovery action; and c. to notify Subscribers as required by the SMKI PMA.	DCC	6.1.3

6.1.3 Post-Recovery

The procedure as set out immediately below shall be used following recovery from the Compromise of a Contingency Private Key or the Contingency Symmetric Key.

Step	When	Obligation	Responsibility	Next Step
6.1.3.1	As soon as reasonably practicable, following completion of the procedure as set out in Section 6.1.2 of this document, as applicable	The DCC shall amend the Anomaly Detection Thresholds for the CS02b Update Security Credentials (anyExceptAbnormalRootByRecovery) Command (where those terms have their GBCS meaning) back to zero (0).	DCC	6.1.3.2

6.1.3.2	As soon as reasonably practicable, following 6.1.3.1	The DCC shall seek instruction from SMKI PMA as to whether to destroy the replaced Contingency Private Key and Contingency Symmetric Key.	DCC	6.1.3.3

6.1.3.3	As soon as reasonably practicable, following 6.1.3.2	The SMKI PMA shall consider the implications and handling instructions for unrecovered Devices and for Devices still in the supply chain. When SMKI PMA is satisfied that it is appropriate to destroy the replaced Contingency Private Key and Contingency Symmetric Key Pair, the SMKI PMA shall instruct the DCC to initiate the destruction process.	SMKI PMA	6.1.3.4

6.1.3.4	As soon as reasonably practicable, following 6.1.3.3	The DCC shall notify the SMKI PMA, via a secured means of: a. whether all the instructions from the SMKI PMA have been successfully completed; b. the number, type and Responsible Supplier associated with the SMETS2+ Devices for which recovery was not successful; c. confirmation that the replaced Contingency Private Key and Contingency Symmetric Key Pair have been destroyed; d. details of any communications received from Users in response to any communication provided by the SMKI PMA; e. details of any Lessons Learned by the DCC from the Recovery Event; and f. the estimated costs of the Recovery Event.	DCC	End of procedure

6.2 Recovery from Compromise of the Recovery Private Key

6.2.1 Pre-Recovery

The DCC shall execute the procedure as set out immediately below, following notification of the Compromise of the Recovery Private Key in accordance with section 3.2 of this document.

Step	When	Obligation	Responsibility	Next Step
6.2.1.1	As soon as reasonably practicable, following notification of the Compromise of the Recovery Private Key, in accordance with section 3.2 of this document	The DCC shall notify the SMKI PMA, via a secured electronic means, as soon as reasonably practicable, that a Compromise, or suspected Compromise, of the Recovery Private Key has been notified. The DCC shall request a decision from the SMKI PMA as to whether recovery should be carried out.	DCC	6.2.1.2
6.2.1.2	As soon as reasonably practicable, following 6.2.1.1	The DCC shall notify each Subscriber to Organisation Certificates, via secured electronic means that the Compromise of the Recovery Private Key has been notified and shall provide details of the affected SMETS2+ Devices and Organisation Certificates, in one or more Other Compromise Notification Files which comply with Appendix D of this document.	DCC	6.2.1.3
6.2.1.3	As soon as reasonably practicable, following 6.2.1.2	The DCC shall take all reasonable steps to provide information to the SMKI PMA to support the SMKI PMA's consideration of what procedural steps (if any) that should be taken in order to recover from the Compromise, where such information may include (but shall not be limited to): a. the number of affected SMETS2+ Devices and Subscribers, which may be provided in one or more Other Compromise Notification Files which comply with	DCC, SMKI PMA	6.2.1.4

		Appendix D of this document; b. the extent to which DCC's monitoring indicates that there has been unauthorised use of the Recovery Private Key; c. the extent to which the vulnerabilities that caused the Compromise have been addressed; d. the steps that DCC reasonably believes should be taken to recover from the Compromise; and e. anticipated timescales for recovery.		
6.2.1.4	As soon as reasonably practicable, following 6.2.1.3	Where the DCC believes that use of the Recovery Private Key is likely to be required by the SMKI PMA, it shall identify such preparatory steps that it considers appropriate and to either take such steps or instruct Parties to take steps as required, including (but not limited to): a. determine the number of Key Custodians required to attend a Key Activation Ceremony for the Recovery Private Key (which may be greater than the minimum number required to activate the Recovery Private Key); b. inform such Key Custodians in respect of the Recovery Private Key, via a secured electronic means, of the date, time and location of a Key Activation Ceremony for the Recovery Private Key; and c. notifying Key Custodians to attend the location at which a relevant Key Generation Ceremony or Key Activation Ceremony may be required; and d. activities required to prepare such systems environment required to support activation and use of the Recovery Private Key.	DCC, Key Custodians	6.2.1.5
6.2.1.5	As soon as reasonably practicable, following 6.2.1.4	The SMKI PMA shall: a. determine which of the steps (if any) as set out in section 4.2.2 of this document should be executed, in order to recover from the Compromise; and b. confirm whether the timescales proposed by the DCC (following consultation with the affected Subscriber(s)) in step 6.2.1.3 for recovery, are approved or whether alternate timescales should apply.	SMKI PMA, DCC	If SMKI PMA determines that no action is required, end of Procedure; otherwise 6.2.1.6

		The SMKI PMA shall inform the DCC of its decision via a secured electronic means.		
6.2.1.6	As soon as reasonably practicable, following 6.2.1.5	The DCC shall notify all Subscribers to Organisation Certificates, by secured electronic means, of the SMKI PMA's decision as to whether or not to execute the recovery procedure (amended as directed) as set out in section 6.2.2.	DCC	Procedure as set out in section 6.2.2 of this document

6.2.2 Execution of Recovery Procedure

The procedure as set out immediately below, amended as instructed by the SMKI PMA in accordance with section 6.2.1 of this document, shall be used when a Recovery Private Key has been Compromised.

Step	When	Obligation	Responsibility	Next Step
6.2.2.1	As soon as reasonably practicable, following confirmation of Compromise and instruction from the SMKI PMA that this recovery procedure should be carried out	Where necessary, the DCC shall temporarily amend the Anomaly Detection Thresholds for the DCC that relate to the issuance of Commands to replace Organisation Certificates on SMETS2+ Devices, to enable replacement of affected Organisation Certificates as notified in section 4.2.1 of this document.	DCC (DSP TAD)	6.2.2.2
6.2.2.2	As soon as reasonably practicable, following 6.2.2.1	The DCC shall: a. determine the number of Key Custodians required to attend a Key Activation Ceremony for the Recovery Private Key (which may be greater than the minimum number required to activate the Recovery Private Key); b. inform such Key Custodians in respect of the Recovery Private Key, via a secured electronic means, of the date, time and location of a Key Activation Ceremony for the Recovery Private Key; and c. participate in the Key Activation Ceremony, in accordance with the Organisation CPS, in order to activate the Recovery Private Key.	DCC, Key Custodians	6.2.2.3

6.2.2.3	As soon as reasonably practicable, following 6.2.2.2	The DCC shall: a. determine the number of Key Custodians required to attend a Key Generation Ceremony for the Recovery Private Key; b. inform such Key Custodians in respect of the Recovery Private Key, via a secured electronic means, of the date, time and location of a Key Generation Ceremony for the Recovery Private Key; and c. participate in the Key Generation Ceremony, as set out in the Organisation CPS, in order to generate a new Recovery Private Key and Recovery Certificate.	DCC, Key Custodians	6.2.2.4
6.2.2.4	As soon as reasonably practicable, following 6.2.2.3	The DCC shall send Commands to all SMETS2+ Devices to replace the Recovery Certificate held on such SMETS2+ Devices with the Recovery Certificate generated in step 6.2.2.3. Such Commands shall include the replacement Recovery Certificate and shall be Digitally Signed using the replaced Recovery Private Key. Once submitted, the DCC shall confirm for each affected SMETS2+ Device that the Command completed successfully and shall generate and maintain records of such confirmations, to support the DCC's confirmation of completion of the recovery procedure.	DCC (as DSP)	6.2.2.5
6.2.2.5	As soon as reasonably practicable, following 6.2.2.4	The DCC shall notify each Responsible Supplier for affected SMETS2+ Devices, by secured electronic means, which SMETS2+ Devices were not recovered successfully, in one or more Other Compromise Recovery Progress Files that comply with Appendix E of this document.	DCC	Procedure as set out in Section 6.2.3 of this document

6.2.3 Post-Recovery

The procedure as set out immediately below shall be used following recovery from the Compromise of a Recovery Private Key, as set out in section 6.2.2 of this document.

Step	When	Obligation	Responsibility	Next Step
6.2.3.1	As soon as reasonably practicable, following completion of the procedure	The DCC shall reinstate its relevant Anomaly Detection Threshold values that were in place immediately prior to the temporary values used during the execution of the procedure set out in this Section 6.2 of this document.	DCC (DSP TAD)	6.2.3.2

	as set out in Section 6.2.2 of this document, as applicable			

6.2.3.2	As soon as reasonably practicable, following 6.2.3.1	The DCC shall consider the Recovery Action Risks before undertaking any of the associated actions. Where the DCC concludes that, at this time, the Recovery Certificates should not be revoked and/or Private Keys not destroyed, the DCC shall inform the SMKI PMA as to the rationale. The DCC may, having considered the Recovery Action Risks, submit Certificate Revocation Requests (CRRs), as set out in the SMKI RAPP, in order to revoke affected Recovery Certificates. The DCC shall revoke Recovery Certificates in accordance with the provisions of Appendix B of the Code and the SMKI RAPP section 8.2. The DCC may, having considered the Recovery Action Risks, destroy the Recovery Private Key associated with the revoked Recovery Certificates.	DCC (as DSP)	6.2.3.3

6.2.3.3	As soon as reasonably practicable, following 6.2.3.2	The DCC shall notify the SMKI PMA, via secured electronic means of: a. whether the recovery from the Compromise has been successfully completed; and b. the number of SMETS2+ Devices for which recovery was not successful, which	DCC	End of procedure

		may be provided in one or more Other Compromise Recovery Progress Files that comply with Appendix E of this document.		

6.3 Recovery from Compromise of the Issuing OCA Private Key

6.3.1 Pre-Recovery

The DCC shall execute the procedure as set out immediately below, following notification of the Compromise of an Issuing OCA Private Key in accordance with section 3.2 of this document.

Step	When	Obligation	Responsibility	Next Step
6.3.1.1	As soon as reasonably practicable, following notification of the Compromise of an Issuing OCA Private Key, in accordance with section 3.2 of this document	The DCC shall notify the SMKI PMA and each Subscriber to affected Organisation Certificates, via a secured electronic means, as soon as reasonably practicable, that a Compromise of an Issuing OCA Private Key has been notified. The DCC shall request a decision from the SMKI PMA as to whether recovery should be carried out.	DCC	6.3.1.2
6.3.1.2	As soon as reasonably practicable, following 6.3.1.1	The DCC shall notify each Subscriber to Organisation Certificates, via secured electronic means, the Compromise of the Issuing OCA Private Key has been notified and shall provide details of the affected SMETS2+ Devices and Organisation Certificates, in one or more Other Compromise Notification files which comply with Appendix D of this document	DCC	6.3.1.3
6.3.1.3	As soon as reasonably practicable, following 6.3.1.2	The DCC shall take all reasonable steps to provide information to the SMKI PMA to support the SMKI PMA's consideration of what procedural steps (if any) that should be taken in order to recover from the Compromise, where such information may include (but shall not be limited to): a. the number of affected SMETS2+ Devices and Subscribers, which may be provided in one or more Other Compromise Notification files which comply with Appendix D of this document; b. the extent to which DCC's monitoring indicates that there has been	DCC, SMKI PMA	6.3.1.4

		unauthorised use of the Issuing OCA Private Key; c. the extent to which the vulnerabilities that caused the Compromise have been addressed; d. the steps that DCC reasonably believes should be taken to recover from the Compromise; e. anticipated timescales for recovery; and f. whether or not DCC is proposing to that multiple Compromises should be dealt with on a common basis and if so why the DCC proposes that they should be so treated.		
6.3.1.4	As soon as reasonably practicable, following 6.3.1.3	Where the DCC believes that use of the Recovery Private Key is likely to be required by the SMKI PMA, it shall identify such preparatory steps that it considers appropriate and to either take such steps or instruct Parties to take steps as required, including (but not limited to): a. determine the number of Key Custodians required to attend a Key Activation Ceremony for the Recovery Private Key (which may be greater than the minimum number required to activate the Recovery Private Key); b. inform such Key Custodians in respect of the Recovery Private Key, via a secured electronic means, of the date, time and location of a Key Activation Ceremony for the Recovery Private Key; c. notifying Key Custodians to attend the location at which a relevant Key Generation Ceremony or Key Activation Ceremony may be required; and d. activities required to prepare such systems environment required to support activation and use of the Recovery Private Key.	DCC, Key Custodians	6.3.1.5
6.3.1.5	As soon as reasonably practicable, following 6.3.1.4	The SMKI PMA shall: a. determine which of the steps (if any) as set out in section 4.2.2 of this document should be executed, in order to recover from the Compromise; and b. confirm whether the timescales proposed by the DCC (following consultation with the affected Subscriber(s)) in step 6.3.1.3	SMKI PMA, DCC	6.3.1.6

		for recovery, are approved or whether alternate timescales should apply. The SMKI PMA shall inform the DCC of its decision via a secured electronic means.		
6.3.1.6	As soon as reasonably practicable, following 6.3.1.5	The DCC shall notify all Subscribers to affected Organisation Certificates, via secured electronic means, of the SMKI PMA's decision as to whether or not to execute the recovery procedure (amended as directed) as set out in section 6.3.2.	DCC	If SMKI PMA determines that no action is required, end of Procedure; otherwise 6.3.1.7
6.3.1.7	As soon as reasonably practicable, following 6.3.1.6	The DCC shall consider the Recovery Action Risks before undertaking any of the associated actions. Where the DCC concludes that, at this time, the Recovery Certificates should not be revoked and / or Private Keys not destroyed, the DCC shall inform the SMKI PMA as to the rationale. Otherwise, the DCC shall revoke the Issuing OCA Certificate to which the affected Issuing OCA Private Key relates, and shall update and lodge the relevant Organisation ARL in the SMKI Repository. The DCC shall destroy the Issuing OCA Private Key that is Compromised or suspected to be Compromised.	DCC (as TSP)	Procedure as set out in Section 6.3.2 of this document

6.3.2 Execution of Recovery Procedure

The procedure as set out immediately below shall be executed in order to recover from the Compromise, or suspected Compromise of an Issuing OCA Private Key, following completion of the procedure as set out in section 6.3.1 of this document.

Step	When	Obligation	Responsibility	Next Step
6.3.2.1	As soon as reasonably practicable, following confirmation of Compromise and instruction from the SMKI PMA that this recovery procedure should be carried out	A SMKI ARO acting on behalf of each affected Subscribers shall, as soon as reasonably practicable, submit an Anomaly Detection Thresholds File to the DCC, which shall include amended Anomaly Detection Thresholds that they estimate will be required to resolve the Compromise. The affected Subscriber shall ensure that the Anomaly Detection Thresholds File is submitted in accordance with the requirements of TADP.	Subscriber	6.3.2.2
6.3.2.2	As soon as reasonably practicable, following 6.3.2.1	The DCC shall temporarily amend the Anomaly Detection Thresholds in accordance with the requirements of TADP, for affected Subscribers to allow submission of Service Requests to replace affected Organisation Certificates on SMETS2+ Devices. The DCC shall inform, via secured electronic means, a SMKI SRO acting and the SMKI ARO that provided the details in step 6.1.2.1, that the Anomaly Detection Threshold values have been successfully amended. The DCC shall amend its Anomaly Detection Thresholds that relate to the issuance of Commands to replace Organisation Certificates on SMETS2+ Devices, to enable replacement of the affected Recovery Certificate on SMETS2+ Devices.	DCC (DSP TAD)	6.3.2.3
6.3.2.3	As soon as reasonably practicable, following 6.3.2.2	The DCC shall generate a new Issuing OCA Key Pair and Issuing OCA Certificate, in accordance with the procedure as set out in the Organisation CPS.	DCC (as TSP)	6.3.2.4
6.3.2.4	As soon as reasonably	The DCC shall: a. determine the number of Key Custodians	DCC, Key Custodians	6.3.2.5

	practicable, following 6.3.2.3	required to attend a Key Generation Ceremony for the relevant Recovery Private Key; b. inform such Key Custodians in respect of the relevant Recovery Private Key, via a secured electronic means, of the date, time and location of a Key Generation Ceremony for the Recovery Private Key; and c. participate in the Key Generation Ceremony, as set out in the Organisation CPS, in order to generate a new Recovery Private Key and Recovery Certificate, Digitally Signed using the new Issuing OCA Private Key.		
6.3.2.5	As soon as reasonably practicable, following 6.3.2.4	The DCC shall: a. determine the number of Key Custodians required to attend a Key Activation Ceremony for the Recovery Private Key (which may be greater than the minimum number required to activate the Recovery Private Key); b. inform such Key Custodians in respect of the Recovery Private Key, via a secured electronic means, of the date, time and location of a Key Activation Ceremony for the Recovery Private Key; and c. participate in the Key Activation Ceremony, in accordance with the Organisation CPS, in order to activate the Recovery Private Key.	DCC, Key Custodians	6.3.2.6
6.3.2.6	As soon as reasonably practicable, following 6.3.2.5	The DCC shall send Commands to all SMETS2+ Devices to replace the Recovery Certificate held on such SMETS2+ Devices with the Recovery Certificate generated in step 6.3.2.4. Such Commands shall include the replacement Recovery Certificate and shall be Digitally Signed using the replaced Recovery Private Key. Once submitted, the DCC shall confirm for each affected SMETS2+ Device that the Command completed successfully and shall generate and maintain records of such confirmations, to support the DCC's confirmation of completion of the recovery procedure. The DCC shall notify each organisation as established in step 6.3.1.3, via a secured electronic means and using one or more Other Compromise Recovery Progress Files that	DCC (as DSP)	6.3.2.7

		comply with Appendix E of this document, of the list of SMETS2+ Devices where the replacement of the Recovery Certificate has been successfully completed.		
6.3.2.7	As soon as reasonably practicable, following 6.3.2.6	Each affected Subscriber shall either: a. identify replacement Organisation Certificates that are not Digitally Signed by the Compromised Issuing OCA Private Key; or b. submit such Certificate Signing Requests (CSRs) that are required in order to acquire new Organisation Certificates that are Digitally Signed by the new Issuing OCA Private Key.	Subscriber	6.3.2.8
6.3.2.8	As soon as reasonably practicable, following 6.3.2.7	Each affected Subscriber shall submit Service Requests, in accordance with the provisions of the DCC User Interface Specification, in order to replace all Organisation Certificates for which it is the Subscriber that are held on SMETS2+ Devices and are signed using the Compromised Issuing OCA Private Key, with new Organisation Certificate as identified in accordance with step 6.3.2.7 that are signed by the new Issuing OCA Private Key that is generated in accordance with step 6.3.2.3. Following attempts to replace affected Organisation Certificates on SMETS2+ Devices, each affected Subscriber shall notify the DCC in respect of replacement of affected Organisation Certificates with new Organisation Certificates, via secured electronic means and in one or more Other Compromise Recovery Progress Files that comply with Appendix E of this document.	Subscriber	6.3.2.9
6.3.2.9	As soon as reasonably practicable, following 6.3.2.8	The DCC shall: a. monitor its records of replacement by affected Subscribers against the list as has been compiled in step 6.3.1.2, to identify successful replacement; b. identify any failures to replace affected Organisation Certificates that have been Digitally Signed using the Issuing OCA Private Key that has been Compromised; and c. monitor revocation of Organisation Certificates that are Digitally Signed using the Compromised Issuing OCA Private Key.	DCC	6.3.2.10

6.3.2.10	As soon as reasonably practicable, following 6.3.2.9	The DCC shall notify each Responsible Supplier for affected SMETS2+ Devices, via secured electronic means and using one or more Other Compromise Recovery Progress Files that comply with Appendix E of this document, the SMETS2+ Devices for which replacement of the Recovery Certificate or affected Organisation Certificates was not successfully completed.	DCC	Procedure as set out in Section 1.1.1 of this document

6.3.3 Post-Recovery

The procedure as set out immediately below shall be used following recovery from the Compromise of an Issuing OCA Private Key.

Step	When	Obligation	Responsibility	Next Step
6.3.3.1	As soon as reasonably practicable, following completion of the procedure as set out in Section 6.3.2 of this document	A SMKI ARO acting on behalf of each affected Subscriber shall, as soon as reasonably practicable, submit appropriate enduring Anomaly Detection Thresholds to the DCC in accordance with the requirements of TADP. The DCC shall amend the relevant Anomaly Detection Thresholds in accordance with the requirements of TADP.	DCC (DSP TAD)	6.3.3.2
6.3.3.2	As soon as reasonably practicable, following 6.3.3.1	The DCC shall notify the SMKI PMA, via a secured electronic means of: a. whether the recovery from the Compromise has been successfully completed; and b. the number of SMETS2+ Devices for which recovery was not successful, which may be provided in one or more Other Compromise Recovery Progress Files that comply with Appendix E of this document.	DCC	End of procedure

7. Replacement of an XML Signing Private Key

The procedures for revoking an Organisation Certificate associated with an XML Signing Private Key that is Compromised is laid out in SEC Appendix D - SMKI RAPP section 8.2.

7.1 XML Signing Private Key destruction considerations

XML Signing Private Keys should not be capable of being used to sign any Commands pursuant to GBCS. In accordance with Section 3.3.1 of Appendix AD of the SEC, it is a requirement on Parties that each XML Signing Private Key must be a separate dedicated Key that is not be used for communication with Devices (i.e. different to that used to sign the GBCS Payload within Signed Pre-Commands). However, this separation is not currently a requirement in relation to DCC.

XML Signing Private Keys should also be different to any other Private Keys within the scope of this document. For Parties, such other Private Keys would have a key usage of key agreement only, as per the Organisation Certificate Policy, and so they cannot be used for any Digital Signature purpose.

Thus, recovery in relation to XML Signing Private Keys should be capable of being independent of other recovery methods. However, if the Compromise, or suspected Compromise, extends to Private Keys whose recovery is dealt with by other sections in this document, careful consideration should be given to the timing and sequencing of those other recovery steps, with steps to destroy XML Signing Private Keys and revoke associated Certificates.

To illustrate with the example of an XML Signing Private Key used by a Supplier Party to sign Service Requests:

Should the XML Signing Private Key be destroyed or the associated Organisation Certificate be revoked prior to either Method 1 or Method 2 recovery on a related Private Key being carried out, this would prevent the User from having Service Requests and Signed Pre-Commands successfully processed by the DCC until the XML Signing Private Key has been replaced and the corresponding replacement Organisation Certificate has been created by the DCC. This is the case even if the Private Key used to Digitally Sign the GBCS Payload held within Signed Pre-Commands has not been destroyed and the corresponding Organisation Certificate has not been revoked.

Therefore, it is important for Subscribers to consider the sequence of Private Key destruction and Organisation Certificate revocation when in such a recovery scenario. Specifically the Subscriber shall consider the Recovery Action Risks before undertaking such steps.

8. Periodic testing of the SMKI Recovery Procedure

8.1 Testing Arrangements

This section describes the DCC's obligations in respect of periodic testing of recovery procedures, in accordance with the provisions of Section L10.1(d) of the Code. At least once every year, the DCC shall:

a) develop a testing plan and a series of testing scenarios which the DCC will conduct in a systems environment which will only be accessible by the DCC, which are representative of the Enrolled Smart Metering Systems and shall take account of any lessons learned from each previous execution of the SMKI Recovery Procedure to recover from a Compromise. The testing plan and testing scenarios will be conducted by the DCC and may include (but shall not be limited to) the following:

i. the means by which Key Custodians are notified and participate in Key Generation Ceremonies and/or Key Activation Ceremonies;

ii. generation of new DCC Key Material, including the Contingency Key Pair, the Recovery Key Pair and the Contingency Symmetric Key used to encrypt the Contingency Public Key;

iii. processes relating to interactions between the DCC and the SMKI PMA in order to determine what steps (if any) should be taken when the use of the Recovery Private Key or Contingency Private Key would be required to recover from a Compromise;

iv. preparation of system environments required to support the SMKI Recovery Procedure;

v. issuance of Commands that are Digitally Signed using the Recovery Private Key and/or Contingency Private Key, and validation that such Commands are successful;

vi. testing of issuance of DCC Alerts following replacement of affected Organisation Certificates in accordance with the SMKI Recovery Procedure; and

vii. transfer of files between DCC and Subscribers to support the execution of the SMKI Recovery Procedure.

b) develop a testing plan and a series of testing scenarios, and conduct such testing scenarios in a systems environment that is available to all Subscribers, which may include (but is not limited to) scenarios a)(vi) and a)(vii) as set out immediately above, along with replacement of Organisation Certificates on SMETS2+ Devices or S1SP Held Device Security Credentials and that are initiated via Service Requests issued by Subscribers.

c) seek input from Subscribers to Organisation Certificates in relation to those testing scenarios that require participation by Subscribers, and take such input into account when proposing and agreeing the testing scenarios with the SMKI PMA;

d) agree such testing scenarios with the SMKI PMA;

e) create test data based upon data collected by the DCC and, where necessary, acquired from Parties;

f) maintain a test environment in order to carry out such periodic testing of the SMKI Recovery Procedure;

g) carry out testing of the SMKI Recovery Procedure for agreed scenarios; and

h) provide a report to the SMKI PMA and Subscribers to Organisation Certificates following periodic testing, which shall detail the success or otherwise of such testing, proposed amendments to the SMKI Recovery Procedure, and any issues arising that require PMA consideration.

In respect of periodic testing of the SMKI Recovery Procedure:

i) SMKI Users shall provide such reasonable assistance to the DCC as is required to support testing; and

j) The SMKI PMA shall review reports from periodic testing and shall direct the DCC, as necessary, to update the SMKI Recovery Procedure.

Appendix A: Communication Formats

In Appendices B to E of this document, each of the CSV files specified shall be encoded using the ASCII character set and:

- must have a comma "," as the field separator;
- must have a line feed character 0x0A as the record separator, which in this section is indicated by the " ▲" character; and

- may include consecutive comma separators to the left of a record separator to specify that a field has a null value. Where this is the case, DCC shall interpret consecutive commas within a record to indicate a null value.

Some spreadsheets output a carriage return line feed 0x0D0A as the record separator for CSV files and/or do not terminate CSV files with a record separator. Each User submitting a CSV file that is to be Digitally Signed using the Private Key associated with a File Signing Certificate shall, prior to Digitally Signing that file, ensure that:

- the CSV file is formatted to ensure that each record has a separator which is a 0x0A character and that any 0x0D character is removed from the file; and

- the CSV file is terminated with a 0x0A character.

Details of the function of the software utility and the method of Digital Signing of files to support the recovery procedures are contained within section 6 of the TADP.

Appendix B: Organisation Compromise Notification File

Due to the differences in the validation mechanisms in the SMETS1 and SMETS2+ system, the terminology used for Organisation Certificates is different. For the purposes of this Appendix, a SMETS1 Notified Critical Supplier/Network Operator Certificate is considered equivalent to a SMETS2+ Supplier/Network Operator Digital Signature Certificate. A Notified Non-Critical Supplier/Network Operator Certificate is equivalent to a Supplier/Network Operator Key Agreement Certificate. On compromise, these Organisation Certificates shall be included in the corresponding parameters in the Notification File. Pre-payment Key Agreement Certificates have no corresponding SMETS1 equivalent. A SMETS1 Supplier does not need to populate this field.

Each Organisation Compromise Notification File shall be in the format set out in this Appendix and shall have a filename of the form:

a) *OC_Priority_UserID_IncidentID_N_FileNum*.csv

Where:

a) *OC* denotes that the file relates an Organisation Compromise.

b) *Priority* contains an integer value which shall be set to a value of 1 or 2, where a lesser value denotes that the file has a higher priority than a file submitted in respect of the same Incident with a Priority field containing a higher value. Where the Subscriber submitting the Organisation Compromise Notification File wishes to apply a priority to Organisation Certificate replacement recovery activities, it shall determine such priority values and include the integer priority value within the filename for each Organisation Compromise Notification File submitted.

c) *UserID* contains the EUI-64 Compliant identifier for:

- the affected Subscriber submitting the file, where an affected Subscriber is submitting the file to the DCC; or

- the Subscriber to which the file is being provided, unless the file is being submitted to the SMKI PMA, where the file is being submitted to a Subscriber by the DCC; or

- the DCC, where the file is being submitted to the SMKI PMA by the DCC.

d) *IncidentID* contains the Incident reference number provided as set out in section 3.2 of this document.

e) *N* denotes that the file is a notification of affected Organisation Certificates and Devices.

f) *FileNum* is an integer value, used to distinguish between data that is split across multiple files due to exceeding the maximum permitted number records per file, which is set out immediately below.

Each Organisation Compromise Notification File shall be generated in accordance with the procedure set out immediately below:

a) an "initial" CSV file shall be created, which shall contain the following records:

- UserID ▲
- Device_ID, Affected_Certificate_Serial_Number_DS,

  Affected_Certificate_Serial_Number_KAK,

  Affected_Certificate_Serial_Number_KAKPP,

  Replacement_Certificate_Serial_Number_DS,

  Replacement_Certificate_Serial_Number_KAK,

  Replacement_Certificate_Serial_Number_KAKPP *(repeated for each affected Device, with no more than 1 million such records permitted within any file, or any larger number of records as directed by the SMKI PMA)* ▲

b) a File Signing Certificate_ID shall be appended to the end of the "initial" file, comprising:

- all of the attributes contained within the 'Issuer' field in the File Signing Certificate, including attribute names, equals signs and values, which shall be encoded in URL format such that it does not contain any special characters, followed by a comma; and
- the Certificate serial number obtained from the 'serialNumber' field in the File Signing Certificate, followed by a 0x0A character; and

c) a Digital_Signature shall be generated from the concatenation of the "initial" CSV file and the File Signing Certificate_ID and appended as a record to the end of the CSV file, in accordance with the procedure set out in Section 6 of the TADP.

Where:

a) The *UserID* field contains the EUI-64 Compliant identifier for:

- the affected Subscriber submitting the file, where an affected Subscriber is submitting the file to the DCC; or
- the Subscriber to which the file is being provided, unless the file is being submitted to the SMKI PMA, where the file is being submitted to a Subscriber by the DCC; or
- the DCC, where the file is being submitted to the SMKI PMA by the DCC.

b) The Device_ID field contains the Device ID.

c) The Affected_Certificate_Serial_Number_DS field contains the Organisation Certificate serial number of the Organisation Certificate affected by the Compromise that is used to populate the Digital Signing Trust Anchor Cell on affected Devices.

d) The Affected_Certificate_Serial_Number_KAK field contains the Organisation Certificate serial number of the Organisation Certificate affected by the Compromise that is used to populate the Key Agreement Key Trust Anchor Cell on affected Devices.

e) The Affected_Certificate_Serial_Number_KAKPP field contains the Organisation Certificate serial number of the Organisation Certificate affected by the Compromise that is used to populate the prepayment Key Agreement Key Trust Anchor Cell on affected Devices. Where the Subscriber that is submitting the file is a Network Party, the Affected_Certificate_Serial_Number_KAKPP field shall not be populated.

f) The Replacement_Certificate_Serial_Number_DS field contains the Organisation Certificate serial number for the Organisation Certificate to be used to populate the Digital Signing Device Trust Anchor Cell. This field shall not be populated where the relevant step of the SMKI Recovery Procedure does not require an affected Subscriber to provide replacement Organisation Certificates that the DCC will use to populate Devices' Trust Anchor Cells using the Recovery Private Key or Contingency Private Key.

g) The Replacement_Certificate_Serial_Number_KAK field contains the Organisation Certificate serial number for the Organisation Certificate to be used to populate the Key Agreement Key Device Trust Anchor Cell. This field shall not be populated where the relevant step of the SMKI Recovery Procedure does not require an affected Subscriber to provide replacement Organisation Certificates that the DCC will use to populate Devices' Trust Anchor Cells using the Recovery Private Key or Contingency Private Key.

h) The Replacement_Certificate_Serial_Number_KAKPP field contains the Organisation Certificate serial number for the Organisation Certificate to be used to populate the prepayment Key Agreement Key Device Trust Anchor Cell. This field shall not be populated where the relevant step of the SMKI Recovery Procedure does not require an affected Subscriber to provide replacement Organisation Certificates that the DCC will use to populate Devices' Trust Anchor Cells using the Recovery Private Key or Contingency Private Key.

i) The File_Signing Certificate_ID field contains the File Signing Certificate ID, which shall not contain a value when the file is issued by the DCC.

j) The Digital_Signature field contains the Digital Signature, which shall not contain a value when the file is issued by the DCC.

Where multiple Organisation Compromise Notification Files are submitted by an affected Subscriber to the DCC in respect of single IncidentID, the DCC shall process the files in order of Priority value, where files with a lower Priority value shall be processed first.

Appendix C: Organisation Compromise Recovery Progress File

Each Organisation Compromise Recovery Progress File shall be in the format set out in this Appendix and shall have a filename of the form:

k) *OC_Priority_UserID_IncidentID_P_FileNum*.csv

Where:

a) *OC* denotes that the file relates an Organisation Compromise.

b) *Priority* contains an integer value which shall be set to 1 or 2, where a lesser value denoting that the file has a higher priority than a file submitted in respect of the same Incident with a Priority field containing a higher value. Such priority values shall have the same value as the corresponding Organisation Compromise Notification File.

c) *UserID* contains the EUI-64 Compliant identifier for:

- the affected Subscriber submitting the file, where an affected Subscriber is submitting the file to the DCC; or

- the Subscriber to which the file is being provided, unless the file is being submitted to the SMKI PMA, where the file is being submitted to a Subscriber by the DCC; or

- the DCC, where the file is being submitted to the SMKI PMA by the DCC.

d) *IncidentID* contains the Incident reference number provided as set out in section 3.2 of this document.

e) *P* denotes that the file is a notification of progress in respect of replacement of affected Certificates and Devices.

f) *FileNum* is an integer value, used to distinguish between data that is split across multiple files due to exceeding the maximum permitted number records per file, which is set out immediately below.

Each Organisation Compromise Recovery Progress File shall be generated in accordance with the procedure set out immediately below:

a) an "initial" CSV file shall be created, which shall contain the following records:

- UserID ▲

- Device_ID, Overall_status, Overall_status_description,

  Affected_Certificate_Serial_Number_DS,

  Affected_Certificate_Serial_Number_KAK,

  Affected_Certificate_Serial_Number_KAKPP,

  Replacement_Certificate_Serial_Number_DS,

  Replacement_Certificate_Serial_Number_KAK,

  Replacement_Certificate_Serial_Number_KAKPP, Replacement_Status_DS, Replacement_Status_KAK, Replacement_Status_KAKPP *(repeated for each affected Device, with no more than 1 million such records permitted within any file, or any larger number of records as directed by the SMKI PMA)* ▲

b) a File Signing Certificate_ID shall be appended to the end of the "initial" CSV file, comprising:

- all of the attributes contained within the 'Issuer' field in the File Signing Certificate, including attribute names, equals signs and values, which shall be encoded in URL format such that it does not contain any special characters, followed by a comma; and

- the Certificate serial number obtained from the 'serialNumber' field in the File Signing Certificate, followed by a 0x0A character; and

c) a Digital_Signature shall be generated from the "initial" CSV file and appended as a record to the end of the CSV file, in accordance with the procedure set out in Section 6 of the TADP.

Where:

a) The UserID field contains the EUI-64 Compliant identifier for:

- the affected Subscriber submitting the file, where an affected Subscriber is submitting the file to the DCC; or

- the Subscriber to which the file is being provided, unless the file is being submitted to the SMKI PMA, where the file is being submitted to a Subscriber by the DCC; or

- the DCC, where the file is being submitted to the SMKI PMA by the DCC.

b) The Device_ID field contains the Device ID.

c) The Overall_status field indicates acceptance or rejection by the DCC of each device identified in the Compromise Notification form

d) The Overall_status_description field indicates the reason for any rejection

e) The Affected_Certificate_Serial_Number_DS field contains the Organisation Certificate serial number of the Organisation Certificate affected by the Compromise that is used to populate the Digital Signing Trust Anchor Cell on affected Devices, where applicable.

f) The Affected_Certificate_Serial_Number_KAK field contains the Organisation Certificate serial number of the Organisation Certificate affected by the Compromise that is used to populate the Key Agreement Key Trust Anchor Cell on affected Devices, where applicable.

g) The Affected_Certificate_Serial_Number_KAKPP field contains the Organisation Certificate serial number of the Organisation Certificate affected by the Compromise that is used to populate the pre-payment Key Agreement Key Trust Anchor Cell on affected Devices, where applicable.

h) The Replacement_Certificate_Serial_Number_DS field contains the Organisation Certificate serial number for the Organisation Certificate to be used to populate the Digital Signing Device Trust Anchor Cell. This field shall not be populated where the relevant step of the SMKI Recovery Procedure does not require an affected Subscriber to provide replacement Organisation Certificates that the DCC will use to populate Devices' Trust Anchor Cells using the Recovery Private Key or Contingency Private Key.

i) The Replacement_Certificate_Serial_Number_KAK field contains the Organisation Certificate serial number for the Organisation Certificate to be used to populate the Key Agreement Key Device Trust Anchor Cell. This field shall not be populated where the relevant step of the SMKI Recovery Procedure does not require an affected Subscriber to provide replacement Organisation Certificates that the DCC will use to populate Devices' Trust Anchor Cells using the Recovery Private Key or Contingency Private Key.

j) The Replacement_Certificate_Serial_Number_KAKPP field contains the Organisation Certificate serial number for the Organisation Certificate to be used to populate the prepayment Key Agreement Key Device Trust Anchor Cell. This field shall not be populated where the relevant step of the SMKI Recovery Procedure does not require an affected Subscriber to provide replacement Organisation Certificates that the DCC will use to populate Devices' Trust Anchor Cells using the Recovery Private Key or Contingency Private Key.

k) The Replacement_Status_DS field contains a value which is one of the permitted response code values for Service Request 6.15.1, as set out in the first column of Table 7 in section 4.1A.3.3 of the Message Mapping Catalogue, in relation to the replacement information from the affected Organisation Certificate in the Digital Signing Trust Anchor Cell on a Device.

l) The Replacement_Status_KAK field contains a value which is one of the permitted response code values for Service Request 6.15.1, as set out in the first column of Table 7 in section 4.1A.3.3 of the Message Mapping Catalogue, in relation to the replacement of information from the affected Organisation Certificate in the Key Agreement Key Trust Anchor Cell on a Device.

m) The Replacement_Status_KAKPP field contains a value which is one of the permitted response code values for Service Request 6.15.1, as set out in the first column of Table 7 in section 4.1A.3.3 of the Message Mapping Catalogue, in relation to the replacement of information from the affected Organisation Certificate in the prepayment Key Agreement Key Trust Anchor Cell on a Device.

n) The File_Signing Certificate_ID field contains the File Signing Certificate ID, which shall not contain a value when the file is issued by the DCC.

o) The Digital_Signature field contains the Digital Signature, which shall not contain a value when the file is issued by the DCC.

Appendix D: Other Compromise Notification File

Each Other Compromise Notification File shall be in the format set out in this Appendix and shall have a filename of the form:

p) *OTH_UserID_IncidentID_N_FileNum*.csv

Where:

a) *OTH* denotes that the file relates to notification of affected Devices for a Compromise not applicable to Appendices B or C of this document.

b) *UserID* contains the EUI-64 Compliant identifier for:

- the Subscriber to which the file is being provided unless the file is being submitted to the SMKI PMA; or

- the EUI-64 Compliant identifier for the DCC where the file is being submitted to the SMKI PMA.

c) *IncidentID* contains the Incident reference number provided as set out in section 3.2 of this document.

d) *N* denotes that the file is a notification of affected Organisation Certificates and Devices.

e) *FileNum* is an integer value, used to distinguish between data that is split across multiple files due to exceeding the maximum permitted number records per file, which is set out immediately below.

Each Other Compromise File shall contain the following records:

a) UserID ▲

b) Device_ID, Affected_Certificate_Serial_Number_Root,

Affected_Certificate_Serial_Number_Recovery,

Affected_Certificate_Serial_Number_Supplier_DS,

Affected_Certificate_Serial_Number_Supplier_KAK,

Affected_Certificate_Serial_Number_Supplier_KAKPP,

Affected_Certificate_Serial_Number_NetworkOperator_DS,

Affected_Certificate_Serial_Number_NetworkOperator_KAK,

Affected_Certificate_Serial_Number_COS_DS,

Affected_Certificate_Serial_Number_WAN_DS,

Replacement_Certificate_Serial_Number_Root,

Replacement_Certificate_Serial_Number_Recovery,

Replacement_Certificate_Serial_Number_Supplier_DS,

Replacement_Certificate_Serial_Number_Supplier_KAK,

Replacement_Certificate_Serial_Number_Supplier_KAKPP,

Replacement_Certificate_Serial_Number_NetworkOperator_DS,

Replacement_Certificate_Serial_Number_NetworkOperator_KAK,

Replacement_Certificate_Serial_Number_COS_DS,

Replacement_Certificate_Serial_Number_WAN_DS *(repeated for each affected Device, with no more than 1 million such records permitted within any file, or any larger number of records as directed by the SMKI PMA)* ▲

Where:

a) The UserID field contains the EUI-64 Compliant identifier for:

- the Subscriber to which the file is being provided unless the file is being submitted to the SMKI PMA; or
- the EUI-64 Compliant identifier for the DCC where the file is being submitted to the SMKI PMA.

b) The Device_ID field contains the Device ID.

c) The Affected_Certificate_Serial_Number_Root field contains the Root OCA Certificate serial number of the Root OCA Certificate affected by the Compromise that is used to populate the Root Trust Anchor Cell on affected Devices, where applicable.

d) The Affected_Certificate_Serial_Number_Recovery field contains the Recovery Certificate serial number of the Recovery Certificate affected by the Compromise that is used to populate the Recovery Trust Anchor Cell on affected Devices, where applicable.

e) The Affected_Certificate_Serial_Number_Supplier_DS field contains the Organisation Certificate serial number of the Organisation Certificate affected by the Compromise that is used to populate the Supplier Digital Signing Trust Anchor Cell on affected Devices, where applicable.

f) The Affected_Certificate_Serial_Number_Supplier_KAK field contains the Organisation Certificate serial number of the Organisation Certificate affected by the Compromise that is used to populate the Supplier Key Agreement Key Trust Anchor Cell on affected Devices, where applicable.

g) The Affected_Certificate_Serial_Number_Supplier_KAKPP field contains the Organisation Certificate serial number of the Organisation Certificate affected by the Compromise that is used to populate the Supplier pre-payment Key Agreement Key Trust Anchor Cell on affected Devices, where applicable.

h) The Affected_Certificate_Serial_Number_NetworkOperator_DS field contains the Organisation Certificate serial number of the Organisation Certificate affected by the Compromise that is used to populate the Network Operator Digital Signing Trust Anchor Cell on affected Devices, where applicable.

i) The Affected_Certificate_Serial_Number_NetworkOperator_KAK field contains the Organisation Certificate serial number of the Organisation Certificate affected by the Compromise that is used to populate the Network Operator Key Agreement Key Trust Anchor Cell on affected Devices, where applicable.

j) The Affected_Certificate_Serial_Number_COS_DS field contains the TCoS Certificate serial number of the TCoS Certificate affected by the Compromise that is used to populate the TCoS Trust Anchor Cell on affected Devices, where applicable.

k) The Affected_Certificate_Serial_Number_WAN_DS field contains the WAN Provider Certificate serial number of the WAN Provider Certificate affected by the Compromise that is used to populate the WAN Provider Trust Anchor Cell on affected Devices, where applicable.

l) The Replacement_Certificate_Serial_Number_Root field contains the Root OCA Certificate serial number for the Root OCA Certificate to be used to populate the Device Root Trust Anchor Cell, where applicable.

m) The Replacement_Certificate_Serial_Number_Recovery field contains the Recovery Certificate serial number for the Recovery Certificate to be used to populate the Device Recovery Trust Anchor Cell, where applicable.

n) The Replacement_Certificate_Serial_Number_Supplier_DS field contains the Organisation Certificate serial number for the Organisation Certificate to be used to populate the Supplier Digital Signing Device Trust Anchor Cell, where applicable.

o) The Replacement_Certificate_Serial_Number_Supplier_KAK field contains the Organisation Certificate serial number for the Organisation Certificate to be used to populate the Supplier Key Agreement Key Device Trust Anchor Cell, where applicable.

p) The Replacement_Certificate_Serial_Number_Supplier_KAKPP field contains the Organisation Certificate serial number for the Organisation Certificate to be used to populate the Supplier prepayment Key Agreement Key Device Trust Anchor Cell, where applicable.

q) The Replacement_Certificate_Serial_Number_NetworkOperator_DS field contains the Organisation Certificate serial number for the Organisation Certificate to be used to populate the Network Operator Digital Signing Device Trust Anchor Cell, where applicable.

r) The Replacement_Certificate_Serial_Number_NetworkOperator_KAK field contains the Organisation Certificate serial number for the Organisation Certificate to be used to populate the Network Operator Key Agreement Key Device Trust Anchor Cell, where applicable.

s) The Replacement_Certificate_Serial_Number_COS_DS field contains the TCoS Certificate serial number for the TCoS Certificate to be used to populate the Device TCoS Trust Anchor Cell, where applicable.

t) The Replacement_Certificate_Serial_Number_WAN_DS field contains the WAN Provider Certificate serial number for the WAN Provider Certificate to be used to populate the Device WAN Provider Trust Anchor Cell, where applicable.

Appendix E: Other Compromise Recovery Progress File

Each Other Compromise Recovery Progress File shall be in the format set out in this Appendix and shall have a filename of the form:

u) *OTH_UserID_IncidentID_P_FileNum*.csv

Where:

a) *OTH* denotes that the file relates to notification of affected Devices for a Compromise not applicable to Appendices B or C of this document.

b) *UserID* contains the EUI-64 Compliant identifier for:

- the Subscriber submitting the file, where a Subscriber is submitting the file to the DCC;
- the Subscriber to which the file is being provided, unless the file is being submitted to the SMKI PMA, where the file is being submitted to the Subscriber by the DCC; or
- the DCC, where the file is being submitted to the SMKI PMA by the DCC.

c) *IncidentID* contains the Incident reference number provided as set out in section 3.2 of this document.

d) *P* denotes that the file is a notification of progress in respect of replacement of affected Certificates and Devices.

e) *FileNum* is an integer value, used to distinguish between data that is split across multiple files due to exceeding the maximum permitted number records per file, which is set out immediately below.

Each Other Compromise File shall be generated in accordance with the procedure set out immediately below:

a) an "initial" CSV file shall be created, which shall contain the following records:

- UserID ▲

  Device_ID, Overall_status, Overall_status_description,

  Replacement_Certificate_Serial_Number_Root,

  Replacement_Certificate_Serial_Number_Recovery,

  Replacement_Certificate_Serial_Number_Supplier_DS,

  Replacement_Certificate_Serial_Number_Supplier_KAK,

  Replacement_Certificate_Serial_Number_Supplier_KAKPP,

  Replacement_Certificate_Serial_Number_NetworkOperator_DS,

  Replacement_Certificate_Serial_Number_NetworkOperator_KAK,

  Replacement_Certificate_Serial_Number_COS_DS,

  Replacement_Certificate_Serial_Number_WAN_DS, Replacement_Status_Root,

  Replacement_Status_Recovery, Replacement_Status_Supplier_DS,

  Replacement_Status_Supplier_KAK, Replacement_Status_Supplier_KAKPP,

  Replacement_Status_NetworkOperator_DS,

  Replacement_Status_NetworkOperator_KAK, Replacement_Status_COS_DS, Replacement_Status_WAN_DS *(repeated for each affected Device, with no more than 1 million such records permitted within any file, or any larger number of records as directed by the SMKI PMA)* ▲

b) a File Signing Certificate_ID shall be appended to the end of the "initial" CSV file, comprising:

- all of the attributes contained within the 'Issuer' field in the File Signing Certificate, including attribute names, equals signs and values, which shall be encoded in URL format such that it does not contain any special characters, followed by a comma; and
- the Certificate serial number obtained from the 'serialNumber' field in the File Signing Certificate, followed by a 0x0A character; and

c) a Digital_Signature shall be generated from the "initial” CSV file and appended as a record to the end of the CSV file, in accordance with the procedure set out in Section 6 of the TADP.

Where:

a) The UserID field contains the EUI-64 Compliant identifier for:

- the Subscriber submitting the file, where a Subscriber is submitting the file to the DCC;
- the Subscriber to which the file is being provided, unless the file is being submitted to the SMKI PMA, where the file is being submitted to the Subscriber by the DCC; or
- the DCC, where the file is being submitted to the SMKI PMA by the DCC.

b) The Device_ID field contains the Device ID.

c) The Overall_status field indicates acceptance or rejection by the DCC of each device identified in the Compromise Notification File

d) The Overall_status_description field indicates the reason for any rejection

e) The Replacement_Certificate_Serial_Number_Root field contains the Root OCA Certificate serial number for the Root OCA Certificate to be used to populate the Device Root Trust Anchor Cell.

f) The Replacement_Certificate_Serial_Number_Recovery field contains the Certificate serial number for the Certificate to be used to populate the Device Recovery Trust Anchor Cell.

g) The Replacement_Certificate_Serial_Number_Supplier_DS field contains the Certificate serial number for the Certificate to be used to populate the Supplier Digital Signing Device Trust Anchor Cell.

h) The Replacement_Certificate_Serial_Number_Supplier_KAK field contains the Certificate serial number for the Certificate to be used to populate the Supplier Key Agreement Key Device Trust Anchor Cell.

i) The Replacement_Certificate_Serial_Number_Supplier_KAKPP field contains the Certificate serial number for the Certificate to be used to populate the Supplier prepayment Key Agreement Key Device Trust Anchor Cell.

j) The Replacement_Certificate_Serial_Number_NetworkOperator_DS field contains the Certificate serial number for the Certificate to be used to populate the Network Operator Digital Signing Device Trust Anchor Cell.

k) The Replacement_Certificate_Serial_Number_NetworkOperator_KAK field contains the Certificate serial number for the Certificate to be used to populate the Network Operator Key Agreement Key Device Trust Anchor Cell.

l) The Replacement_Certificate_Serial_Number_COS_DS field contains the Certificate serial number for the Certificate to be used to populate the Device TCoS Trust Anchor Cell.

m) The Replacement_Certificate_Serial_Number_WAN_DS field contains the Certificate serial number for the Certificate to be used to populate the Device WAN Provider Trust Anchor Cell.

n) The Replacement_Status_Root field contains a value which is one of the permitted response code values for Service Request 6.15.1, as set out in the first column of Table 7 in section 4.1A.3.3 of the Message Mapping Catalogue, in relation to the replacement of information from the affected Certificate in the Root Trust Anchor Cell on a Device.

o) The Replacement_Status_Recovery field contains a value which is one of the permitted response code values for Service Request 6.15.1, as set out in the first column of Table 7 in section 4.1A.3.3 of the Message Mapping Catalogue, in relation to the replacement of information from the affected Certificate in the Recovery Trust Anchor Cell on a Device.

p) The Replacement_Status_Supplier_DS field contains a value which is one of the permitted response code values for Service Request 6.15.1, as set out in the first column of Table 7 in section 4.1A.3.3 of the Message Mapping Catalogue, in relation to the replacement of information from the affected Certificate in the Supplier Digital Signing Trust Anchor Cell on a Device.

q) The Replacement_Status_Supplier_KAK field contains a value which is one of the permitted response code values for Service Request 6.15.1, as set out in the first column of Table 7 in section 4.1A.3.3 of the Message Mapping Catalogue, in relation to the replacement of information from the affected Certificate in the Supplier Key Agreement Key Trust Anchor Cell on a Device.

r) The Replacement_Status_Supplier_KAKPP field contains a value which is one of the permitted response code values for Service Request 6.15.1, as set out in the first column of Table 7 in section 4.1A.3.3 of the Message Mapping Catalogue, in relation to the replacement of information from the affected Certificate in the Supplier prepayment Key Agreement Key Trust Anchor Cell on a Device.

s) The Replacement_Status_NetworkOperator_DS field contains a value which is one of the permitted response code values for Service Request 6.15.1, as set out in the first column of Table 7 in section 4.1A.3.3 of the Message Mapping Catalogue, in relation to the replacement of information from the affected Certificate in the Network Operator Digital Signing Trust Anchor Cell on a Device.

t) The Replacement_Status_NetworkOperator_KAK field contains a value which is one of the permitted response code values for Service Request 6.15.1, as set out in the first column of Table 7 in section 4.1A.3.3 of the Message Mapping Catalogue, in relation to the replacement of information from the affected Certificate in the Network Operator Key Agreement Key Trust Anchor Cell on a Device.

u) The Replacement_Status_COS_DS field contains a value which is one of the permitted response code values for Service Request 6.15.1, as set out in the first column of Table 7 in section 4.1A.3.3 of the Message Mapping Catalogue, in relation to the replacement of information from the affected Certificate in the TCoS Trust Anchor Cell on a Device.

v) The Replacement_Status_WAN_DS field contains a value which is one of the permitted response code values for Service Request 6.15.1, as set out in the first column of Table 7 in section 4.1A.3.3 of the Message Mapping Catalogue, in relation to the replacement of information from the affected Certificate in the WAN Provider Trust Anchor Cell on a Device.

w) The File_Signing Certificate_ID field contains the File Signing Certificate ID, which shall not contain a value when the file is issued by the DCC.

x) The Digital_Signature field contains the Digital Signature, which shall not contain a value when the file is issued by the DCC.

Appendix F: Definitions

Term	Definition
Chief Information Security Officer	Means a senior security officer within a Party who is responsible for activities including (but not limited to) establishing and maintaining the security vision, strategy, information security governance framework, secure asset and infrastructure control framework, and security risk management program
Data Services Provider, or DSP	Means the DCC acting from those systems identified in part a) of the definition of DCC Live Systems
DSP Threshold Anomaly Detection, or DSP TAD	Means the DCC acting using those systems identified in Part (b) of the definition of DCC Live Systems
Key Activation Ceremony	Means a meeting at which a Private Key or Symmetric Key is activated by the DCC and/or Key Custodians, such that the Private Key or Symmetric Key may be used
Key Generation Ceremony	Means a meeting at which a Private Key or Contingency Symmetric Key is generated by the DCC and Key Custodians
Key Component	Means part of a Key or part of Activation Data used to protect a Key.
Key Custodian	Means an individual, appointed in accordance with section 3.4 of the SMKI Recovery Procedure, to hold a key which may be used as part of the process to access a Key Component.
Organisation Compromise Notification File	A CSV file used to support recovery from a Compromise that is specified in Appendix B of the SMKI Recovery Procedure
Organisation Compromise Recovery Progress File	A CSV file used to support recovery from a Compromise that is specified in Appendix C of the SMKI Recovery Procedure
Other Compromise Notification File	Means a CSV file used to support recovery from a Compromise that is specified in Appendix D of the SMKI Recovery Procedure
Other Compromise Recovery Progress File	Means a CSV file used to support recovery from a Compromise that is specified in Appendix E of the SMKI Recovery Procedure
S1SP Held Device Security Credentials	Means, in relation to a SMETS1 Device and as the context requires, any or all of the Notified Critical Supplier Certificate, the Notified Non-Critical Supplier Certificate, the Notified Critical Network Operator Certificate and the Notified Non-Critical Network

	Operator Certificate, in each case as defined in Appendix AM of the SEC (SMETS1 Supporting Requirements).

Trust Anchor Cell	Shall have its GBCS meaning.

Trusted Service Provider, or TSP	Means the DCC acting using systems identified in part (d) of the definition of DCC Live Systems

wrappedApexContingency Key	Means the value used in the `WrappedApexContingencyKey` extension (with the meaning of IETF RFC 5934 section 9) in a Root OCA Certificate

Appendix G: SMKI Recovery Procedure Test Scenarios

Each scenario set out in this Appendix G can be tested in isolation, or combined as part of a more extensive test.

9.1 DCC and SMKI PMA Interactions

These scenarios cover the testing of interactions between the DCC Service Desk and the SMKI PMA in the event of a (suspected) Compromise.

ID	SMKI 200

Title:	Notification of (suspected) Compromise and SMKI PMA Response

Description	DCC service Desk completes Compromise Notification Report DCC service Desk communicates Compromise Notification Report DCC Service Desk requests SMKI PMA Decision (not applicable to the Method 1 of the Organisation Recovery process) SMKI PMA acknowledge receipt of Compromise Notification Report SMKI PMA provides instruction / guidance to the DCC through the DCC Service Desk in response to the Compromise Notification Report as to whether Recovery should be carried out and if so, which steps of the chosen approach

Objective	• To prove DCC processes in regard to the Compromise Notification Report preparation • To prove communication of (suspected) Compromise process to the SMKI PMA by the DCC Service Desk • To prove SMKI PMA instruction / guidance to the DCC Service Desk processes • To prove SMKI PMA decision making processes in response to the Compromise Notification Report and request for guidance / instruction

ID	SMKI 201

Title:	Notification of outcome of Recovery processes

Description	DCC Service Desk prepares Organisation Compromise Recovery Report for the SMKI PMA DCC Service Desk communicates Recovery Report to the SMKI PMA SMKI PMA acknowledges receipt of Organisation Compromise Recovery Report

Objective	• To prove DCC processes for the preparation of the Organisation Compromise Recovery Report • To prove communication of the Organisation Compromise Recovery Report to the SMKI PMA by the DCC Service Desk • To prove SMKI PMA processes in respect of receipt of the Organisation Compromise Recovery Report

9.2 DCC / Subscriber and DCC / Party Interactions and Processes

9.2.1 Organisation Certificate Revocation and Replacement

ID	SMKI 214

Title:	Organisation Certificate Revocation

Descriptio n	Subscriber submits Certificate Revocation Request(s) (CRR) through the DCC Service Desk DCC revokes Organisation Certificates identified in the CRR(s) DCC Service Desk communicates outcome of Revocation request to Subscriber

Objective	• To prove Subscriber processes in response to a (suspected) Compromise of one its Organisation Private Keys • To prove DCC and Subscriber interactions to revoke an Organisation Certificate

ID	SMKI 202

Title:	Replacement Organisation Certificates

Descriptio n	Subscriber obtains new or identifies existing Organisation Certificates to replace on affected Devices or those that form a part of any S1SP Held Device Security Credentials Subscriber communicates decision in the form of a Certificate ID to the DCC through the DCC Service Desk

Objective	• To prove, during the Recovery process, that the Subscriber can request new Organisation Certificates or identify and obtain existing Organisation Certificates to be placed on affected Devices, or the notification of the Certificate ID to the DCC where they form a part of any S1SP Held Device Security Credentials. • To prove Subscriber communications with the DCC Service Desk in respect of the replacement Organisation Certificates

9.2.2 Communication of SMKI PMA Decision to Subscriber

ID	SMKI 203

Title:	DCC Communicates SMKI PMA Recovery Decision to Subscriber

Descriptio n	DCC Service Desk communicates the decision of the SMKI PMA in respect of whether Recovery will be used and if so, which methods and steps are to be carried out

Objective	• To prove DCC Service Desk and Subscriber interactions in respect of SMKI PMA decisions

9.2.3 Subscriber notification of Compromise

ID	SMKI 215
Title:	Send DCC Organisation Notification and Anomaly Detection Threshold changes
Descriptio n	Subscriber / Supplier submits through the DCC Service Desk Organisation Compromise Notification Files or Other Compromise Notification Files and Anomaly Detection Thresholds amendments for the purposes of Recovery, in accordance with the TADP
Objective	• To prove Subscriber / Supplier processes and interactions with the DCC Service Desk in regard to the submission of information relating to impacted devices, incident • To prove Subscriber / Supplier processes and interactions with the DCC Service Desk in regard to the temporary amendment of Anomaly Detection Thresholds to support Recovery

ID	SMKI 216
Title:	Threshold Anomaly Detection – Post-recovery – applies to Method 1 of Organisation Certificate Recovery from Compromise only
Descriptio n	Subscriber / Supplier submits through the DCC Service Desk Anomaly Detection Thresholds for re-instatement following recovery
Objective	• To prove Subscriber / Supplier processes and interactions with the DCC Service Desk in regard to the re-instigation of Anomaly Detection Thresholds following Recovery

ID	SMKI 217
Title:	DCC amends Anomaly Detection Thresholds
Descriptio n	DCC amends Anomaly Detection Thresholds in response to Recovery process to enable communications to Devices to be processed by the DSP DCC informs Subscriber of Threshold Anomaly Detection value change
Objective	• To prove DCC processes in respect of Threshold Anomaly Detection value change during Recovery • To prove DCC and Subscriber interactions in respect of Threshold Anomaly Detection value change during Recovery

ID	SMKI 218

Title:	DCC re-instates Anomaly Detection Thresholds

Descriptio n	DCC Service Desk amends Anomaly Detection Thresholds to those set before the Recovery process commenced DCC Service Desk informs Anomaly Detection Thresholds change

Objective	• To prove DCC processes in respect of Anomaly Detection Thresholds reinstatement following Recovery • To prove DCC and Subscriber interactions in respect of Anomaly Detection Thresholds reinstatement during Recovery

9.2.4 DCC Notification to Parties other than the (suspected) Compromised Subscriber

ID	SMKI 204

Title:	Method 1, Method 1A and Method 3 – Responsible Supplier Notification of (suspected) Compromise

Descriptio n	DCC Service Desk identifies affected Devices for which the Subscriber is not the Responsible Supplier DCC Service Desk notifies Responsible Supplier(s) for those Devices using Organisation Compromise Notification file

Objective	• To prove DCC Service Desk and Responsible Supplier processes with regard to notification of (suspected) Compromise to Responsible Suppliers for Devices which are affected by the (suspected) Compromise

ID	SMKI 205

Title:	Method 1, Method 1A and Method 3 - Responsible Supplier Notification of Progress / Outcome of Recovery

Descriptio n	DCC Service Desk identifies affected Devices for which the Subscriber is not the Responsible Supplier DCC Service Desk notifies Responsible Supplier(s) for those Devices using Organisation Compromise Progress file and therefore the cessation of communications with affected Devices during Recovery

Objective	• To prove DCC Service Desk and Party processes with regard to notification of progress of Recovery to Responsible Suppliers for Devices which are affected by the (suspected) Compromise

ID	SMKI 206

Title:	Method 2 – Network Operator Notification of (suspected) Compromise

Descriptio n	DCC Service Desk identifies Network Operators for affected Devices reported by the Subscriber DCC Service Desk notifies using the Organisation Notification file Network Operators for those Devices of the Subscriber's intent to Recover using Method 2 and cessation of communications during Recovery

Objective	• To prove DCC Service Desk and Network Operator Party processes with regard to notification of (suspected) Compromise to Network Operators for Devices which are affected by the (suspected) Compromise

ID	SMKI 207

Title:	Method 2 – Network Operator Notification of Progress / Outcome of Recovery

Descriptio n	DCC Service Desk identifies Network Operators for affected Devices reported by the Subscriber DCC Service Desk notifies Network Operator(s) for those Devices of Recovery progress / outcome of Recovery using the Organisation Compromise Progress file

Objective	• To prove DCC Service Desk and Network Operator Party processes with regard to notification of progress of Recovery to Network Operators for Devices which are affected by the (suspected) Compromise

9.3 Method 1 - Subscriber Service Requests and Alert Responses

This scenario is applicable only to Method 1 of the Recovery of Organisation Certificate held on a Device (section 4.1 of the SMKI Recovery Procedures). Its execution will be through the combination of individual test scenarios as set out above in section 8.2 of this Appendix G.

ID	SMKI 208

Title:	Method 1 - Subscriber Recovers using own Private Key

Descriptio n	Subscriber sends Service Requests to replace Organisation Certificates on affected Devices, signed using its own private key which is the subject of the (suspected) Compromise Subscriber monitors progress of Recovery through Alerts received from affected Devices in response to the instruction to replace Organisation Certificates Subscriber informs DCC through DCC Service Desk of the progress of Recovery through an Organisation Compromise Progress Report File

Objective	• **To prove Subscriber processes in response to a (suspected) Compromise of one its Organisation Private Keys**

9.4 Method 1A Compromise of any S1SP Held Device Security Credentials

This scenario is applicable only to Method 1A to recover from a Compromise of the Private Key associated with the Public Key contained within an Organisation Certificate that forms part of any S1SP Held Device Security Credentials, in accordance with section 3.2 and 4.1A of this document.

ID	SMKI 208A

Title:	**Method 1A -Subscriber Recovers using own Private Key**

Description	**Subscriber sends Service Requests to replace Organisation Certificates that form a part of any S1SP Held Device Security Credentials, signed using its own private key which is the subject of the Compromise** **Subscriber monitors progress of Recovery through Alerts received from the SMETS1 Service Provider in response to the instruction to replace Organisation Certificates** **Subscriber informs DCC through DCC Service Desk of the progress of Recovery through an Organisation Compromise Progress Report File**

Objective	• **To prove Subscriber processes in response to a Compromise of one its Organisation Private Keys related to an Organisation Certificate that forms a part of any S1SP Held Device Security Credentials**

9.5 Methods 2 & 3 – Communications with affected Devices in Response to the Supplier / Subscribers Service Requests

These scenarios are applicable to Methods 2 and / or 3 of the Recovery of Organisation Certificate held on a Device (section 4.1A of the SMKI Recovery Procedures). Their execution will be through the combination of individual test scenarios as set out above in section 8.2 of this Appendix G.

ID	SMKI 209

Title:	**Suspension of Communications with Devices**

Descriptio n	**DCC suspends communications to Devices where the Compromise impacts Supplier and / or Communication Service Provider Certificates on those Devices** **DCC confirms decision of the SMKI PMA with regard to the suspension or if reinstates communication according to the decision of the SMKI PMA**

Objective	• **To prove DCC Service Desk and DCC processes with regard to the suspension of communications with affected Devices**

ID	SMKI 210

Title:	Set status of affected Devices to Recovery

Description	Where the affected Subscriber is not a Network Provider, DCC sets status in the Smart Metering Inventory of affected Devices to 'Recovery'

Objective	• To prove DCC Service Desk and DCC processes with regard to the SMI status change during Recovery processes

ID	SMKI 211

Title:	Commands sent to affected Devices to effect Recovery – Method 2 only

Description	DCC issues Commands as set out in the GBCS signed with the Recovery Private Key and containing ACB Certificates as the replacement Supplier Certificate DCC monitor for Alerts received from Devices and forwards the Alert to the affected Supplier DCC sets SMI status of affected Devices that have reported successful Recovery to 'Recovered' DCC notifies affected Subscriber of progress of the Recovery Processes using the DCC Alert and Organisation Recovery Progress file Supplier Issues Service Requests to replace the ACB Certificate in the Supplier slot with a new Supplier Certificate DCC processes these Service Requests Supplier notifies the outcome of Supplier Certificate Replacement using the Organisation Recovery Progress file DCC sets SMI status of the Device to the pre-Recovery State on receipt of the Response from the Device indicating successful Certificate Update

Objective	• To prove DCC and DCC Service Desk processes during Method 2 of Organisation Certificate Recovery • To prove Suppliers processes during Method 2 of Organisation Certificate Recovery • To prove interactions between Supplier and DCC Service Desk during Method 2 of Organisation Certificate Recovery

ID	SMKI 213

Title:	Commands sent to affected Devices to effect Recovery – Method 3 only

Description	DCC issues Commands as set out in the GBCS signed with the Recovery Private Key and containing the Certificate identified by the Subscriber as the replacement Certificate DCC monitor for Alerts received from Devices and forwards the Alert to the affected Subscriber DCC sets SMI status of affected Devices that have reported successful certificate replacement to the pre-recovery status DCC notifies affected Subscriber of progress of the Recovery Processes using the Organisation Recovery Progress file DCC notifies the Device's Responsible Supplier (if not the Subscriber) of failed certificate replacement events using the Organisation Recovery Progress file

Objective	• To prove DCC and DCC Service Desk processes during Method 3 of Organisation Certificate Recovery • To prove Subscribers processes during Method 3 of Organisation Certificate Recovery • To prove interactions between Subscribers and DCC Service Desk during Method 3of Organisation Certificate Recovery • To prove interactions between Responsible Suppliers and DCC Service Desk during Method 3 of Organisation Certificate Recovery

9.6 End to End Tests

These Test Scenarios constitute full Tests of each Recovery Process set out in the sections 4 and 6 of the SMKI Recovery Procedures. It is intended that these tests are carried out periodically as set out in section 7.1 of this SMKI Recovery Procedures.

ID	SMKI 101

Title:	Recovery from Compromise of an Organisation Private Key (other than the Recovery Private Key) – Method 1 and Method 1A

Descriptio n	As set out in section 4.1 and 4.1A of the SMKI Recovery Procedures (except for the standing-up of the Recovery Environment)

Objective	• To prove in an end to end test the processes to Recover from the Compromise of an Organisation Private Key (other than the Recovery Private Key) – Method 1 and Method 1A

ID	SMKI 102

Title:	Recovery from Compromise of an Organisation Private Key (other than the Recovery Private Key) – Method 2

Descriptio n	As set out in section 4.2 of the SMKI Recovery Procedures (except for the standing-up of the Recovery Environment)

Objective	• To prove in an end to end test the processes to recover from the Compromise of an Organisation Private Key (other than the Recovery Private Key) – Method 2

ID	SMKI 103

Title:	Recovery from Compromise of an Organisation Private Key (other than the Recovery Private Key) – Method 3

Descriptio n	As set out in section 4.3 of the SMKI Recovery Procedures (except for the standing-up of the Recovery Environment)

Objective	• To prove in an end to end test the processes to recover from the Compromise of an Organisation Private Key (other than the Recovery Private Key) – Method 3

ID	SMKI 104

Title:	Recovery from Compromise of a Recovery Private Key

Description	As set out in section 6.2 of the SMKI Recovery Procedures (except for the standing-up of the Recovery Environment)

Objective	• To prove in an end to end test the processes to recover from the Compromise of the Recovery Private Key

ID	SMKI 105

Title:	Recovery from Compromise of an Issuing OCA Private Key

Description	As set out in section 6.3 of the SMKI Recovery Procedures (except for the standing-up of the Recovery Environment)

Objective	• To prove in an end to end test the processes to recover from the Compromise of an Issuing OCA Private Key

ID	SMKI 106

Title:	Recovery from Compromise of a Contingency Private Key or the Contingency Symmetric Key

Description	As set out in section 6.1 of the SMKI Recovery Procedures

Objective	• To prove in an end to end test the processes to recover from the Compromise of a Contingency Private Key or Contingency Symmetric Key

Version: M6.0

Appendix M

SMKI Interface Design Specification

Contents

1 Introduction

1.1 Purpose

Section L4 of the Code sets out the obligation on the DCC to maintain the SMKI Service Interface in accordance with the SMKI Interface Design Specification. Section L4.4 sets out the content of the SMKI Interface Design Specification including the protocols and technical standards which are all based on open standards and defines the technical details of the interfaces to SMKI Services insofar as they relate to Authorised Subscribers.

1.2 Target Response Times

For the purposes of supporting the measurement of Target Response Times in accordance with Section L8.3 of the Code, the terms “sending” and “receipt” should be interpreted as follows:

a) for the Ad Hoc Device CSR Web Service interface:

   i. “receipt” means the receipt of a Device CSR in the DCC Systems that is submitted by an Authorised Subscriber via the Ad Hoc Device CSR Web Service interface, following successful completion by DCC of all verification and validation checks as set out in the SMKI Interface Design Specification in relation to ad hoc Device CSRs submitted through the Ad Hoc Device CSR Web Service interface; and

   ii. “sending” means the submission of a Device Certificate or CSR processing error messages from the DCC Systems to the Authorised Subscriber within the synchronous response to the corresponding request; or

b) for the Batched Device CSR Web Service interface:

   i. “receipt” means the receipt of a Batched Certificate Signing Request (Batched CSR) in the DCC Systems that is submitted by an Authorised Subscriber via the Batched Device CSR Web Service interface, following successful completion by DCC of all verification and validation checks as set out in the SMKI Interface Design Specification in relation to Batched CSRs submitted through the Batched Device CSR Web Service interface; and

   ii. “sending” means making available the files containing Device Certificates and/or CSR processing error messages via the Batched Device CSR Web Service interface, for download by the Authorised Subscriber; or

c) for a Batched CSR via the SMKI Portal interface (via DCC Gateway Connection):

i. “receipt” means the receipt of a Batched CSR in the DCC Systems that is submitted by an Authorised Subscriber via the SMKI Portal interface, following successful completion by DCC of all verification and validation checks as set out in the SMKI Interface Design Specification in relation to Batched CSRs submitted through the SMKI Portal interface; and

ii. “sending” means making available the files containing Device Certificates and/or CSR processing error messages on the SMKI Portal interface, for download by the Authorised Subscriber; or

d) for an ad hoc Device CSR via the SMKI Portal interface (via DCC Gateway Connection):

i. “receipt’ means the receipt of an ad hoc Device CSR in the DCC Systems that is submitted by an Authorised Subscriber via the SMKI Portal interface following successful completion by DCC of all validation and verification checks set out in the SMKI Interface Design Specification in relation to ad hoc Device CSRs submitted through the SMKI Portal interface; and

ii. “sending” means making available the Device Certificate or CSR processing error messages on the SMKI Portal interface, for download by the Authorised Subscriber.

e) for an Organisation CSR via the SMKI Portal interface (via DCC Gateway Connection or via the Internet):

i. “receipt’ means the receipt of an Organisation CSR in the DCC Systems that is submitted by an Authorised Subscriber via the SMKI Portal interface following successful completion by DCC of all validation and verification checks set out in the SMKI Interface Design Specification in relation to Organisation CSRs; and

ii. “sending” means making the Organisation Certificate or CSR processing error messages on the SMKI Portal interface, for download by the Authorised Subscriber.

2 SMKI interfaces

2.1 Interface Definition

The DCC shall make the following interfaces available, in order that Authorised Subscribers may access the SMKI Services.

In accordance with the SMKI Code of Connection, the DCC shall make four interfaces available to Parties and RDPs:

a) a SMKI Portal interface, accessed via an Authorised Subscriber’s web browser and only accessible via a DCC Gateway Connection (as set out in Section 2.3 of this document);

b) an Ad Hoc Device CSR Web Service interface, for the purposes of submitting single Device CSRs, that may be accessed by an Authorised Subscriber’s automated systems, and only accessible via the DCC Gateway Connection (as set out in Section 2.4 of this document);

c) a Batched Device CSR Web Service interface, for the purposes of submitting Batched CSRs for Device Certificates, that may be accessed by an Authorised Subscriber’s automated systems, and only accessible via the DCC Gateway Connection (as set out in Section 2.5 of this document); and

d) a SMKI Portal interface made available over a secured Internet connection and accessed through an Authorised Subscriber’s web browser that does not use a DCC Gateway Connection (as set out in Section 2.6 of this document).

2.2 General obligations

The DCC shall ensure that PKCS#10 certification request standard is used for the submission of Certificate Signing Requests (CSRs). Authorised Subscribers shall submit Certificate Signing Requests according to the CSR structures as defined in Appendix F of this document.

In accordance with Sections L11.5 - L11.7 of the SEC, unless an Authorised Subscriber immediately notifies the DCC of Certificate rejection, the Certificate shall be deemed to be accepted.

The DCC shall ensure that the URLs of the interfaces to SMKI Services shall remain unchanged in the event of the failure of a component of interfaces to the SMKI Services, or invocation of business continuity or disaster recovery measures. The DCC shall ensure that disaster recovery systems are functionally identical to the main interface.

Error codes and examples of error messages in relation to:

a) the SMKI Portal interface via DCC Gateway Connection and SMKI Portal interface via the Internet are set out in the SMKI User Guide;

b) the Ad Hoc Device CSR Web Service interface are set out in Appendix A of this document; and

c) the Batched Device CSR Web Service interface are set out in Appendix C and Appendix D of this document.

2.3 SMKI Portal interface via DCC Gateway Connection

General obligations

The SMKI Portal interface via DCC Gateway Connection provides an asynchronous mechanism for Authorised Responsible Officers (AROs) to submit Organisation CSRs, and Device CSRs in batch or ad-hoc form on behalf of their Authorised Subscriber.

The DCC shall ensure that the SMKI Portal interface via DCC Gateway Connection:

a) uses the HTTPS protocol, secured by mutually authenticated TLS in line with the cryptographic standards set out in Appendix G of this document;

b) uses Javascript, Cascading Style Sheets (CSS) and images;

c) is compliant with the W3C "Web Content Accessibility Guidelines" (v2) at "AA" level; and

d) is only accessible using a DCC Gateway Connection.

The process for obtaining a DCC Gateway Connection is detailed in Section H15 of the Code.

Establishing a secured web browser connection to the SMKI Portal interface via DCC Gateway Connection

In order to establish a secured web browser connection to the SMKI Portal interface via DCC Gateway Connection, an Authorised Subscriber shall:

a) access the SMKI Portal landing page via a defined URL (as set out in the SMKI User Guide), which shall be secured using HTTPS;

b) then select the relevant link to access the SMKI Portal page supplied to enable submission and retrieval of Organisation CSRs/Certificates or Device CSRs/Certificates; and

c) having selected the relevant link in b), ensure the web browser connection is secured by establishing a mutually authenticated TLS session by entering the PIN code used to enable use of the relevant Cryptographic Credential Token, and presenting the IKI Certificate (which has been Issued in accordance with the SMKI RAPP for the purposes of accessing the SMKI Portal via DCC Gateway Connection) to the DCC for either:

Authorised Subscribers for Organisation Certificates, for the purposes of submitting Organisation CSRs and retrieval of resulting Organisation Certificates; or

Authorised Subscribers for Device Certificates, for the purposes of submitting Device CSRs and retrieval of resulting Device Certificates.

In order for a secured web browser connection to the SMKI Portal interface via DCC Gateway Connection to be established, the DCC shall ensure that the SMKI Portal via DCC Gateway Connection presents to the user a x.509 v3 certificate that is recognised by the CA/Browser Forum for the purposes of allowing the Authorised Subscriber's web browser to validate and authenticate the DCC's server as part of establishing the mutually authenticated TLS session.

The DCC shall ensure that the SMKI Portal via DCC Gateway Connection denies access where the user does not present a valid IKI Certificate for authentication.

Submission of Organisation CSRs and retrieval of resulting Organisation Certificates

2.3.1.1 Submission of Organisation CSRs by Authorised Subscriber

Subject to the provisions of 2.3.1.1 A, Authorised Subscribers wishing to be issued with an Organisation Certificate shall ensure that they:

a) generate a relevant CSR in line with Appendix F of this document, and Appendix B of the Code; and

b) paste the CSR (formatted in line with Appendix F of this document) into the Certificate Signing Request form and then submit the CSR, via the SMKI Portal interface.

A. Network Parties who are Authorised Subscribers accessing the SMKI Portal via the Internet may optionally elect not to populate the value field of the "Subject Unique Identifier" with a 64 bit EUI-64 Compliant identifier, in which case:

a) they shall leave the value field of the "Subject Unique Identifier" blank, and otherwise proceed in accordance with the requirements of 2.3.1.1 (b);

b) a submission made in accordance with 2.3.1.1 A(a) shall be treated for the purposes of the Code (including this Appendix M) as a CSR and be processed accordingly by the DCC, provided that:

c) the Authorised Subscriber must subsequently provide a human readable hexadecimal representation of the EUI-64 value to be included within the Certificate (so using 0..9, a..f, A..F) to the DCC through the SMKI Portal interface via the Internet and re-submit the fully completed CSR via that interface;

d) the DCC shall ensure that a suitably authorised member of Registration Authority personnel confirms that:

i. the representation of the EUI-64 Compliant identifier that has been provided is a representation of an EUI-64 Compliant identifier that has been allocated by the SEC Panel to the Authorised Subscriber, and

ii. the Authorised Subscriber is a Network Party, and in either case, if not, the DCC shall not Issue an Organisation Certificate to the Authorised Subscriber.

B. The provisions of 2.3.1.1 A shall not apply until such time as the DCC notifies the Security Sub-Committee that the DCC Systems capability to support the provisions of 2.3.1.1 A has been adequately tested and is ready to be used.

C. Following a notification from the DCC to the Security Sub-Committee in accordance with the provisions of 2.3.1.1 B, sub-Clause 2.3.1.1 B and this sub-Clause 2.3.1.1 C shall automatically be deleted from this Appendix M.

2.3.1.2 Receipt and validation of Organisation CSRs by the DCC

Following receipt by the DCC of an Organisation CSR, the DCC shall:

a) validate the format, and verify the Digital Signature of the CSR in line with Appendix F of this document and PKCS#10; and

b) either accept, or reject the CSR;

i. where the CSR is accepted, return a notification via the SMKI Portal interface of acceptance to the Authorised Subscriber; or

ii. where the CSR is rejected, log an error and return an error message via the SMKI Portal interface to the Authorised Subscriber.

2.3.1.3 Actions following acceptance of Organisation CSRs by the DCC

Where an Organisation CSR is accepted, the DCC shall:

a) verify the content of the CSR, which shall include checking that the EUI-64 Compliant identifier contained in the CSR relates to an Authorised Subscriber on whose behalf the Authorised Responsible Officer submitting the CSR is authorised to submit CSRs; and

b) either approve the CSR for further processing or reject the CSR;

i. where the CSR is approved, return a notification via the SMKI Portal interface of acceptance to the Authorised Subscriber; or

ii. where the CSR is rejected, notify the Authorised Subscriber via the SMKI Portal interface of the errors and reasons for the rejection of that CSR.

If an Organisation CSR is rejected by the DCC, the Authorised Subscriber must, if they still wish to be issued with a relevant Organisation Certificate, correct the errors and re-submit the CSR. The Authorised Subscriber does not need to generate a new Key Pair in respect of the Organisation CSR.

2.3.1.4 Actions following approval of Organisation CSRs by the DCC

Where an Organisation CSR is approved by the DCC, the DCC shall:

a) Issue a corresponding Organisation Certificate;

b) lodge the resulting Organisation Certificate in the SMKI Repository; and

c) make the Organisation Certificate available for download via the SMKI Portal interface via DCC Gateway Connection and the SMKI Repository.

2.3.1.5 Actions following download of an Organisation Certificate by an Authorised Subscriber

Upon downloading the Issued Organisation Certificate, the Authorised Subscriber shall in accordance with L11.5 of the Code, establish that the information contained in the resulting Organisation Certificate is consistent with the information contained in the corresponding Organisation CSR.

Should there be an inconsistency, the Authorised Subscriber shall immediately reject the Organisation Certificate in accordance with L11.5 by notifying the DCC via the Service Desk, and inform the DCC of the inconsistency. Should the DCC be notified by an Authorised Subscriber of an inconsistency, the DCC shall log the event and investigate as appropriate.

Upon rejection of the Organisation Certificate by an Authorised Subscriber and subsequent notification to the DCC of such rejection, the DCC shall revoke the Organisation Certificate, place the Organisation Certificate on the Organisation CRL, and lodge the updated Organisation CRL in the SMKI Repository in accordance with Appendix B of the Code.

Submission of Device CSRs (Ad Hoc or Batched) and retrieval of resulting Device Certificates

A Device Certificate can be submitted through the SMKI Portal interface via DCC Gateway Connection in ad hoc Device CSR form or as a number in Batched CSR form.

2.3.1.6 Submission of an ad hoc Device CSR or Batched CSR by Authorised Subscriber

Authorised Subscribers wishing to be issued with a Device Certificate or Device Certificates shall ensure that they generate the relevant Device CSRs in line with Appendix F of this document, and Appendix A of the Code.

a) **Ad Hoc Device CSR submission** - where the Authorised Subscriber wishes to submit an ad hoc Device CSR, the Authorised Subscriber shall paste the CSR into the ad hoc Device CSR form (as set out in the SMKI User Guide) and then submit it to the SMKI Portal interface; or

b) **Batched CSR submission -** where the Authorised Subscriber wishes to submit a Batched CSR, the Authorised Subscriber shall:

   i. generate the relevant Device CSRs; and

ii. create a .zip file containing the individual Device CSRs, formatted in line with Appendix F of this document, then upload and submit the .zip file using the Batched CSR web form (as set out in the SMKI User Guide) to the SMKI Portal interface.

2.3.1.7 Receipt and validation of Device CSR (Ad Hoc or Batched) by the DCC

Following receipt by the DCC of an ad hoc Device CSR or Batched CSR to the SMKI Portal via DCC Gateway Connection, the DCC shall:

a) for an ad hoc Device CSR submission:

i. validate the format, and verify the Digital Signature of the CSR in line with Appendix F of this document and PKCS#10;

ii. apply the Eligible Subscriber checks as set out in Section L3.16 of the Code; and

iii. either accept, or reject the CSR; and

A. where the CSR is accepted, return a notification via the SMKI Portal interface of acceptance to the Authorised Subscriber; or

B. where the CSR is rejected, log an error and return an error message that is in accordance with “Response Status” table in Appendix A of this document, via the SMKI Portal interface to the Authorised Subscriber; or

b) for a Batched CSR submission:

i. validate that the structure of the submitted .zip file is in accordance with the format set out in Appendix F to this document;

ii. validate that the number of CSRs contained within the Batched CSR is less than or equal to 50,000;

A. should the Batched CSR contain more than 50,000 CSRs, the DCC shall reject the Batched CSR (including all of the Device CSRs contained within the Batched CSR); or

B. should the Batched CSR contain less than or equal to 50,000 CSRs, further validate the Batched CSR as set out below;

iii. either accept, or reject the Batched CSR and/or each constituent Device CSR, log relevant errors and return a synchronous response via the SMKI Portal interface to notify the Authorised Subscriber as to:

A. where the Batched CSR is accepted, acceptance of the Batched CSR and the number of Device CSRs submitted within the Batched CSR; or

B. where the Batched CSR is rejected, relevant error messages that are in accordance with "Response Status" table in Appendix C of this document.

2.3.1.8 Actions following acceptance of Device CSRs by the DCC

If a Device CSR is accepted, the DCC shall:

a) for an ad hoc Device CSR submission:

i. perform such additional checks as DCC determines is necessary on the Device CSR, which may include checking that all mandatory fields are present and conform to the requirements set out in the Device Certificate Policy;

ii. check that less than 100 Device Certificates have previously been Issued for the Device ID to which the Device CSR relates;

iii. either approve, or reject the Device CSR; and

A. where the CSR is accepted, return a notification via the SMKI Portal interface of acceptance to the Authorised Subscriber; or

B. where the CSR is rejected, log an error that is in accordance with "Response Status" table in Appendix A of this document, and return an error message via the SMKI Portal interface to the Authorised Subscriber; or

b) for a Batched CSR submission:

i. validate the format, and verify the signature of each Device CSR contained within the Batched CSR in line with Appendix F of this document and PKCS#10;

ii. perform such additional checks as DCC determines is necessary on one or more of the Device CSRs in the Batched CSR, which may include checking that all mandatory fields are present and conform to the requirements set out in the Device Certificate Policy;

iii. apply the Eligible Subscriber checks as set out in Section L3.16 of the Code;

iv. check that less than 100 Device Certificates have previously been Issued for the Device ID to which each Device CSR relates;

v. either approve, or reject each Device CSR in the Batched CSR; and

A. where the CSR is approved, include a notification in the Batched CSR response file, as set out in section 2.3.1.9d) of this document, to the Authorised Subscriber; or

B. where the CSR is rejected, log an error that is in accordance with "Response Status" table in Appendix C of this document, and include an error notification in the Batched CSR response file, as set out in section 2.3.1.9d) of this document.

Where a CSR has been rejected by the DCC because it would breach the 100 Device Certificate limit, the Authorised Subscriber should contact the Service Desk in order to review with the DCC the threshold applying in relation to the particular Device ID such that additional Device Certificates may be issued in relation to it.

If a Device CSR is rejected by the DCC, including where contained within a Batched CSR, the Authorised Subscriber must, if they still wish to be issued with a relevant Device Certificate, correct the errors and re-submit the CSR. The Authorised Subscriber may not need to instruct the Device to generate a new Key Pair for the subsequent CSR depending on the error condition.

2.3.1.9 Actions following approval of Device CSRs by the DCC

Where a Device CSR is approved by the DCC, the DCC shall:

a) Issue a corresponding Device Certificate;

b) lodge the resulting Device Certificate in the SMKI Repository; and

c) for ad hoc Device CSRs:

i. make the corresponding Device Certificate, for up to 30 days following provision by the DCC, available for download via the 'certificate pickup' page on the SMKI Portal interface via DCC Gateway Connection (as set out in the SMKI User Guide) and the SMKI Repository;

In order to retrieve the Device Certificate, the Authorised Subscriber will establish a connection to the SMKI Portal interface via DCC Gateway Connection using the IKI Certificate Issued for the purposes of submitting Device CSRs and retrieving Device Certificates; or

d) for Batched CSRs:

i. make available, for up to 30 days following provision by the DCC, two files for download via the 'certificate pickup' page on the SMKI Portal interface, comprising:

A. a .zip file containing the Certificates in Base64 encoded DER format resulting from successfully processed CSRs; and

B. a .txt file containing a report showing the processed status of each CSR in the Batched CSR, including errors.

In order to retrieve the response files (as set out above) which correspond with a Batched CSR submission, the Authorised Subscriber will establish a connection to the SMKI Portal interface via DCC Gateway Connection using the IKI Certificate Issued for the purposes of submitting Device CSRs and retrieving Device Certificates.

2.3.1.10 Actions following download of a Device Certificate by an Authorised Subscriber

Upon downloading the Issued Device Certificate, the Authorised Subscriber shall, in accordance with L11.6, take reasonable steps to establish that the information contained in the resulting Device Certificate is consistent with the information contained in the corresponding Device CSR.

Should there be an inconsistency, the Authorised Subscriber shall immediately reject the Device Certificate in accordance with L11.6 by notifying the DCC via the Service Desk, and inform the DCC of the inconsistency. Should the DCC be notified by an Authorised Subscriber of an inconsistency, the DCC shall log the event and investigate as appropriate.

2.4 Ad Hoc Device CSR Web Service interface

General obligations

The Ad Hoc Device CSR Web Service interface provides a synchronous mechanism for an Authorised Subscriber’s systems to submit individual Device CSRs.

The DCC shall ensure that the Ad Hoc Device CSR Web Service interface:

a) is only accessible to Authorised Subscribers for Device Certificates acting on behalf of Parties in the User Role of either Import Supplier or Gas Supplier, or the DCC;

b) uses the HTTPS protocol, secured by mutually authenticated TLS, in line with the cryptographic properties set out in Appendix G of this document;

c) uses Extensible Markup Language (XML) over REST for Device CSR message requests and responses;

d) provides message responses which are consistent with Appendix A of this document;

e) uses the XML schema for CSR message requests and responses defined in Appendix B of this document; and

f) is only accessible using a DCC Gateway Connection.

Prior to gaining access to the Ad Hoc Device CSR Web Service interface, Authorised Subscribers shall prepare and provide to the DCC a CSR, as set out in Appendix G, in electronic form in respect of an IKI Certificate in accordance with the procedures set out in the SMKI RAPP section 5.4 and as set out immediately below.

The DCC shall validate the format, and verify the signature of the CSR in line with Appendix G of this document and the IKI Certificate Policy. If accepted, the DCC shall process the CSR and shall, if accepted, provide the Authorised Subscriber with the following, in accordance with the SMKI RAPP section 5.4:

a) an IKI Certificate issued under the appropriate IKI Certification Authority for the purpose of enabling client authentication to the Ad Hoc Device CSR Web Service interface; and

b) a CA/Browser Forum recognised certification authority root certificate and all corresponding issuing authority certificates, for the purposes of enabling server authentication of the Ad Hoc Device CSR Web Service interface.

Establishing a secured connection to the Ad Hoc Device CSR Web Service interface

In order to establish a secured TLS connection to the Ad Hoc Device CSR Web Service interface, an Authorised Subscriber for Device Certificates acting as an Import Supplier or Gas Supplier, or the DCC, shall:

a) configure its system(s) to connect to the Ad Hoc Device CSR Web Service interface URL, as set out in the SMKI User Guide;

b) establish a TLS session by presenting the IKI Certificate which has been Issued in accordance with the SMKI RAPP for the purposes of TLS mutual authentication to secure access to the Ad Hoc Device CSR Web Service interface; and

c) configure its systems such that the TLS session renegotiation timeout is set to 5 minutes for each connection to the Ad Hoc Device CSR Web Service interface.

In order for a secured connection to the Ad Hoc Device CSR Web Service interface to be established, the DCC shall ensure that the Ad Hoc Device CSR Web Service presents the CA/Browser Forum certificate referenced in the ‘General obligations’ part of section 2.4 of this document, for the purposes of allowing the Authorised Subscriber’s systems to authenticate the server as part of establishing the mutually authenticated TLS session.

The DCC shall ensure that access to the Ad Hoc Device CSR Web Service interface is denied where the user does not present a valid IKI Certificate for authentication.

Submission of Device CSRs and retrieval of resulting Device Certificates

2.4.1.1 Submission of Device CSRs by Authorised Subscriber

Authorised Subscribers wishing to be Issued with a Device Certificate via the Ad Hoc Device CSR Web Service interface shall ensure that they:

a) generate a Device CSR in line with Appendix F of this document and Appendix A of the Code; and

b) include the Device CSR in the XML format defined in the XML schema set out in Appendix B of this document and submit the CSR via HTTP POST to the Ad Hoc Device CSR Web Service interface.

2.4.1.2 Receipt and validation of Device CSRs by the DCC

Following receipt of a Device CSR to the Ad Hoc Device CSR Web Service interface, the DCC shall:

a) validate that the format of the XML document complies with the XML schema as set out in Appendix B of this document;

b) validate the format, and verify the Digital Signature of the CSR in line with Appendix F of this document and PKCS#10;

c) either accept, or reject the CSR; and

   i. where the CSR is rejected, log an error and return an error message in the synchronous XML response, to the Authorised Subscriber's systems.

2.4.1.3 Actions following acceptance of Device CSRs by the DCC

If a Device CSR is accepted, the DCC shall:

a) check that at least one Key Agreement Certificate or Digital Signing Certificate has previously been Issued for the Device ID to which the Device CSR relates;

b) check that less than 100 Device Certificates have previously been Issued for the Device ID to which the Device CSR relates;

c) either approve, or reject the Device CSR; and

   i. where the CSR is approved, return a notification of acceptance in the synchronous XML response, to the Authorised Subscriber's systems; or

   ii. where the CSR is rejected, log an error and return an error message in the synchronous XML response, to the Authorised Subscriber's systems.

2.4.1.4 Actions following approval of Device CSRs by the DCC

Where a Device CSR submitted via the Ad Hoc Device CSR Web Service interface is approved, the DCC shall:

a) Issue a corresponding Device Certificate;

b) lodge the resulting Device Certificate in the SMKI Repository; and

c) return the Device Certificate to the Authorised Subscriber, as set out in Appendix A to this document, in the synchronous XML response to the submission of the Device CSR via the Ad Hoc Device CSR Web Service interface.

2.4.1.5 Actions following download of a Device Certificate by an Authorised Subscriber

Upon downloading or viewing the Issued Device Certificate, the Authorised Subscriber shall, in accordance with L11.6, take reasonable steps to establish that the information contained in the resulting Device Certificate is consistent with the information contained in the corresponding Device CSR.

Should there be an inconsistency, the Authorised Subscriber shall immediately reject the Device Certificate in accordance with L11.6 by notifying the DCC via the Service Desk, and inform the DCC of the inconsistency. Should the DCC be notified by an Authorised Subscriber of an inconsistency, the DCC shall log the event and investigate as appropriate.

2.5 Batched Device CSR Web Service interface

General obligations

The Batched Device CSR Web Service interface provides a synchronous mechanism for an Authorised Subscriber’s systems to submit Batched CSRs containing Device CSRs and subsequently a synchronous mechanism to retrieve the resulting Device Certificates.

The DCC shall ensure that the Batched Device CSR Web Service interface:

a) uses the HTTPS protocol, secured by mutually authenticated TLS, in line with the cryptographic properties set out in Appendix G of this document;

b) uses Extensible Markup Language (XML) over REST for Batched CSR message requests, Batched CSR responses and provision of Device Certificates;

c) provides message responses corresponding with submission of Batched CSRs which are consistent with Appendix C of this document;

d) provides message responses in relation to the processing of individual Device CSRs that are contained within a Batched CSR which are consistent with Appendix D of this document;

e) uses the XML schema for Batched CSR message requests and responses defined in Appendix E; and

f) is only accessible using a DCC Gateway Connection.

Prior to gaining access to the Batched Device CSR Web Service interface, an Authorised Subscriber for Device Certificates shall prepare and provide to the DCC a CSR, as set out in Appendix G, in electronic form in respect of an IKI Certificate in accordance with the procedures set out in the SMKI RAPP section 5.4.

The DCC shall validate the format, and verify the signature of the CSR in line with Appendix G of this document and the IKI Certificate Policy. If accepted, the DCC shall process the CSR and shall, if accepted, provide the following in accordance with the SMKI RAPP:

a) an IKI Certificate issued under the appropriate IKI Certification Authority enabling authentication to the Batched Device CSR Web Service interface; and

b) a CA/Browser Forum recognised certification authority root certificate and all corresponding issuing authority certificates for the purposes of enabling server authentication of the Batched Device CSR Web Service interface.

Establishing a secured connection to the Batched Device CSR Web Service interface

In order to establish a connection to the Batched Device CSR Web Service interface, an Authorised Subscriber for Device Certificates shall:

a) configure its system(s) to connect to the Batched Device CSR Web Service interface URL, as set out in the SMKI User Guide;

b) establish a TLS session by presenting an IKI Certificate Issued in accordance with the SMKI RAPP for the purposes of TLS mutual authentication in order to secure access to the Batched Device CSR Web Service interface; and

c) configure its system(s) such that the TLS session renegotiation timeout is set to 5 minutes.

The DCC shall ensure that the Batched Device CSR Web Service presents the CA/Browser Forum certificate referenced in the ‘General obligations’ part of section 2.5 of this document, for the purposes of allowing the Authorised Subscriber’s client to authenticate the DCC’s server as part of establishing the mutually authenticated TLS session.

The DCC shall ensure that access to the Batched Device CSR Web Service interface is denied where the user does not present a valid IKI Certificate for authentication.

Submission of Batched CSRs and retrieval of resulting Device Certificates

2.5.1.1 Submission of Batched CSRs by Authorised Subscriber

An Authorised Subscriber wishing to be Issued with Device Certificates in response to a Batched CSR submission via the Batched Device CSR Web Service interface shall ensure that it:

a) generates each CSR to be contained within the Batched CSR in line with Appendix F of this document and Appendix A of the Code;

b) include each Device CSR in the Batched CSR in the XML format defined in the XML schema set out in Appendix E of this document; and

c) submit the XML document containing the Batched CSR via HTTP POST to the Batched Device CSR Web Service interface.

2.5.1.2 Receipt and validation of Batched CSR by the DCC

On receipt of an XML document containing a Batched CSR to the Batched Device CSR Web Service interface from an Authorised Subscriber's system, the DCC shall:

a) validate that the format of the XML document complies with the XML schema as set out in Appendix E of this document;

b) validate that the number of CSRs contained within the Batched CSR is less than or equal to 50,000;

    i. should the Batched CSR contain more than 50,000 CSRs, the DCC shall reject the Batched CSR (including all of the Device CSRs contained within the Batched CSR); or

    ii. should the Batched CSR contain less than or equal to 50,000 CSRs, further validate the Batched CSR as set out below;

c) either accept, or reject the Batched CSR, log relevant errors and return in the synchronous XML response to the Authorised Subscriber's systems, to notify the Authorised Subscriber as to:

where the Batched CSR is accepted, acceptance of the Batched CSR;

where the Batched CSR is rejected, relevant error messages; and

a Batched CSR identifier that can be used to retrieve the Batched CSR XML response file as set out in section 2.5.1.4 of this document.

2.5.1.3 Actions following acceptance of Device CSRs in a Batched CSR by the DCC

Upon acceptance of a Batched CSR as set out immediately above, the DCC shall:

a) validate the format, and verify the Digital Signature of each CSR in line with Appendix F of this document and PKCS#10;

b) perform such additional checks as DCC determines is necessary on one or more of the Device CSRs in the Batched CSR, which may include checking that all mandatory fields are present and conform to the requirements set out in the Device Certificate Policy;

c) apply the Eligible Subscriber checks as set out in Section L3.16 of the Code;

d) check that less than 100 Device Certificates have previously been Issued for the Device ID to which each Device CSR relates;

e) either approve, or reject each Device CSR in the Batched CSR and include (where applicable) resulting Device Certificates, notifications and error messages in a Batched CSR XML response file that is separate from the synchronous response file described in section 2.5.1.2 of this document; and

   i. where the CSR is approved, include a notification in the Batched CSR XML response file, to the Authorised Subscriber; or

   ii. where the CSR is rejected, log an error and include an error notification in the Batched CSR XML response file.

Where a CSR has been rejected by the DCC because it would breach the 100 Device Certificate limit, the Authorised Subscriber should contact the Service Desk in order to review with the DCC the threshold applying in relation to the particular Device ID such that additional Device Certificates may be issued in relation to it.

If a Device CSR is rejected by the DCC, including where contained within a Batched CSR, the Authorised Subscriber must, if they still wish to be issued with a relevant Device Certificate, correct the errors and re-submit the CSR. The Authorised Subscriber may not need to instruct the Device to generate a new Key Pair for the subsequent CSR depending on the error condition.

2.5.1.4 Actions following approval of Device CSRs in a Batched CSR by the DCC

Where a Device CSR submitted via the Batched CSR Web Service interface is approved, the DCC shall:

a) Issue a corresponding Device Certificate;

b) lodge the resulting Device Certificate in the SMKI Repository;

c) make the Device Certificate available to the Authorised Subscriber for download in the Batched CSR XML response file, as described in section 2.5.1.3, Appendix D and Appendix E to this document; and

d) generate files for download via the ‘certificate pickup’ page on the SMKI Portal interface, as set out in section 2.3.1.9 of this document.

An Authorised Subscriber may, at any point up to 30 days following provision by the DCC, download the XML response file containing success and error information and Device Certificates Issued in response to Device CSRs in a Batched CSR, by:

a) establishing a TLS mutual authentication session to the Batched Device CSR Web Service interface; and

b) appending the Batched CSR identifier supplied in response to the Batched CSR submission to the URL as defined in the SMKI User Guide for the purposes of retrieving response XML files for Batched CSR submissions.

2.5.1.5 Actions following download of a Device Certificate by an Authorised Subscriber

Upon downloading or viewing the Issued Device Certificate, the Authorised Subscriber shall, in accordance with L11.6, take reasonable steps to establish that the information contained in the resulting Device Certificate is consistent with the information contained in the corresponding Device CSR.

Should there be an inconsistency, the Authorised Subscriber shall immediately reject the Device Certificate in accordance with L11.6 by notifying the DCC via the Service Desk, and inform the DCC of the inconsistency. Should the DCC be notified by an Authorised Subscriber of an inconsistency, the DCC shall log the event and investigate as appropriate.

2.6 SMKI Portal interface via the Internet

General obligations

The SMKI Portal interface via the Internet provides an asynchronous mechanism for Authorised Responsible Officers (AROs) not accessing the SMKI Service through a DCC Gateway Connection to submit Organisation CSRs and to retrieve resulting Certificates, on behalf of their Authorised Subscriber.

The SMKI Portal via the Internet also provides a mechanism by which Authorised Subscribers may access certain SMKI Repository content.

The DCC shall ensure that the SMKI Portal interface via the Internet:

a) uses the HTTPS protocol, secured by mutually authenticated TLS in line with the cryptographic standards set out in Appendix G of this document;

b) uses Javascript, Cascading Style Sheets (CSS) and images;

c) is compliant with the W3C “Web Content Accessibility Guidelines” (v2) at “AA” level;

d) provides a separate static URL, as set out in the SMKI User Guide, enabling SMKI Portal interface users to download a file in .zip format as defined in Appendix F to this document, updated as necessary, containing the base set of Organisation Certificates and OCA Certificates required to populate Device anchor slots prior to installation for the north Region;

e) provides a separate static URL, as set out in the SMKI User Guide, enabling SMKI Portal interface users to download a file in .zip format as defined in Appendix F to this document, updated as necessary, containing the base set of

Organisation Certificates and OCA Certificates required to populate Device anchor slots prior to installation for the central Region and south Region;

f) provides a static URL, as set out in the SMKI User Guide, enabling SMKI Portal interface users to download the latest IKI CRL;

g) provides a static URL, as set out in the SMKI User Guide, enabling SMKI Portal interface users to download the latest Organisation CRL;

h) provides a static URL, as set out in the SMKI User Guide, enabling SMKI Portal interface users to download the latest IKI ARL;

i) provides a static URL, as set out in the SMKI User Guide, enabling SMKI Portal interface users to download the latest Organisation ARL;

j) provides a web form, as set out in the SMKI User Guide, where persons with access to the SMKI Portal via the Internet can request information held within the SMKI Repository. The DCC shall process such requests and provide information via electronic means; and

k) is only accessible via the Internet.

Provision of a connection to the Internet is the responsibility of the Authorised Subscriber.

The DCC shall ensure that the Organisation Certificates and OCA Certificates contained within the two Device anchor slot Certificate files shall be the same, other than the Organisation Certificates required to populate the WAN provider Device anchor slot.

The DCC shall lodge a document in the SMKI Repository, which sets out details of which of the base set of Organisation Certificates and OCA Certificates may be placed in specific Device anchor slots.

Establishing a secured web browser connection to the SMKI Portal interface via the Internet

In order to establish a connection to the SMKI Portal interface via the Internet, an Authorised Subscriber shall:

access a SMKI Portal landing page via defined URL (as defined in the SMKI User Guide) which shall be secured using HTTPS;

then select the relevant link to access the SMKI Portal page supplied to enable submission and retrieval of Organisation CSRs/Certificates; and

having selected the relevant link in b), ensure the web browser connection is secured by establishing a mutually authenticated TLS session by entering the PIN code used to enable use of the relevant Cryptographic Credential Token, and presenting an IKI Certificate (which has been Issued in accordance with the SMKI RAPP for the purposes of accessing the SMKI Portal via the Internet) to the DCC for Authorised Subscribers for Organisation Certificates, for the purposes of submitting Organisation CSRs and retrieval of resulting Organisation Certificates.

In order for a secured web browser connection to the SMKI Portal interface via the Internet to be established, the DCC shall ensure that the SMKI Portal via the Internet presents to the user a x.509 v3 certificate that is recognised by the CA/Browser Forum for the purposes of allowing the Authorised Subscriber's systems to authenticate the server as part of establishing the mutually authenticated TLS session.

The DCC shall ensure that the SMKI Portal via the Internet denies access where the user does not present a valid IKI Certificate for authentication.

Submission of Organisation CSRs and retrieval of resulting Organisation Certificates

2.6.1.1 Submission of Organisation CSRs by Authorised Subscriber

Authorised Subscribers wishing to be issued with an Organisation Certificate shall ensure that they:

a) generate a relevant CSR in line with Appendix F of this document, and Appendix B of the Code; and

b) paste the CSR (formatted in line with Appendix F of this document) into the Certificate Signing Request form and then submit the CSR, via the SMKI Portal interface.

2.6.1.2 Receipt and validation of Organisation CSRs by the DCC

Following receipt of an Organisation CSR, the DCC shall:

a) validate the format, and verify the Digital Signature of the CSR in line with Appendix F of this document and PKCS#10;

b) either accept, or reject the CSR:

   i. where the CSR is accepted, return a notification via the SMKI Portal interface of acceptance to the Authorised Subscriber; or

   ii. where the CSR is rejected, log an error and return an error message via the SMKI Portal interface to the Authorised Subscriber.

2.6.1.3 Actions following acceptance of Organisation CSRs by the DCC

Where an Organisation CSR is accepted, the DCC shall:

a) verify the content of the CSR, which shall include checking that the EUI-64 Compliant identifier contained in the CSR relates to an Authorised Subscriber on whose behalf the Authorised Responsible Officer submitting the CSR is authorised to submit CSRs; and

b) either approve the CSR for further processing or reject the CSR;

i. where the CSR is approved, return a notification via the SMKI Portal interface of acceptance to the Authorised Subscriber; or

ii. where the CSR is rejected, notify the Authorised Subscriber via the SMKI Portal interface of the errors and reasons for the rejection of that CSR.

If an Organisation CSR is rejected by the DCC, the Authorised Subscriber must, if they still wish to be issued with a relevant Organisation Certificate, correct the errors and re-submit the CSR. The Authorised Subscriber does not need to generate a new Key Pair in respect of the Organisation CSR.

2.6.1.4 Actions following approval of Organisation CSRs by the DCC

Where an Organisation CSR is approved by the DCC, the DCC shall:

a) process the CSR;

b) Issue a corresponding Organisation Certificate;

c) lodge the resulting Organisation Certificate in the SMKI Repository; and

d) make the Organisation Certificate available for download via the SMKI Portal interface via the Internet and the SMKI Repository.

2.6.1.5 Actions following download of an Organisation Certificate by an Authorised Subscriber

Upon downloading the Issued Organisation Certificate, the Authorised Subscriber shall in accordance with L11.5 of the Code, establish that the information contained in the resulting Organisation Certificate is consistent with the information contained in the corresponding Organisation CSR.

Should there be an inconsistency, the Authorised Subscriber shall immediately reject the Organisation Certificate in accordance with L11.5 by notifying the DCC via the Service Desk, and inform the DCC of the inconsistency. Should the DCC be notified by an Authorised Subscriber of an inconsistency, the DCC shall log the event and investigate as appropriate.

Upon rejection of the Organisation Certificate by an Authorised Subscriber and subsequent notification to the DCC of such rejection, the DCC shall revoke the Organisation Certificate, place the Organisation Certificate on the Organisation CRL, and lodge the updated CRL in the SMKI Repository in accordance with Appendix B of the Code.

Appendix A Ad-Hoc Device CSR Web Service Messages

Example: Device Certificate Signing Request Message

The following message format is used to request a Device Certificate from SMKI via the Ad Hoc Device CSR Web Service interface.

```
Host: localhost:443
Content-Length: 439
User-Agent: Jakarta Commons-HttpClient/3.0.1
Content-Type: application/xml;charset=UTF-8

<?xml version="1.0” encoding=”utf-8”?>
 <DeviceCertificateSigningRequest ID="clientId1">
 <Version>1.0</Version>
<CertificateSigningRequest>MIIBDTC………HULdtQN</CertificateSigningRequest>
</DeviceCertificateSigningRequest>
```

Device Certificate Signing Request: Element Table

Element Name	*Description*
DeviceCertificateSigningRequest	*The root element*
Version	*This element contains the version of the Ad Hoc Device CSR Web Service interface. In the schema specified in Appendix B of this document, this value is set to “1.0”*
CertificateSigningRequest	*This element contains the ‘base64text’ field (as defined in RFC 7468 section 3) of the PKCS#10 Certificate Signing Request (CSR) without whitespace. The element shall NOT contain the ‘preeb’ and ‘posteb’ fields.*

Device Certificate Signing Request: Attribute Table

Attribute Name	*Description*
ID	*The client reference to the request. This value will be returned in the response unless the original request is incorrectly formed.*

Example: Response to Ad Hoc Device Certificate Signing Request – Success

The following message is returned in response to Device Certificate Signing Request when the DCC has successfully Issued a Device Certificate. The message includes the Device Certificate that was Issued.

```
HTTP/1.1 200 OK
Date: Tue, 13 May 2014 12:15:58 GMT
Content-Length: 362
Content-Type: application/xml;charset=UTF-8
Server: Apache-Coyote/1.1

<?xml version="1.0” encoding=”utf-8”?>
<DeviceCertificateSigningResponse ID="clientid1">
        <Version>1.0</Version>
        <Build>1.1.4</Build>
        <TransactionId>12345</TransactionId>
        <Status>SUCCESS</Status>
<Certificate>MIAGCSqGSIb3DQEHA………AAAAAA</Certificate>
</DeviceCertificateSigningResponse>
```

Example: Response to Ad Hoc Device Certificate Signing Request – Incorrect XML

The following message is returned in response to invalidly formed Device CSR. Where there is an invalidly formed Device CSR, the DCC may be unable to return the client supplied ID value.

```
HTTP/1.1 200 OK
Date: Tue, 13 May 2014 12:15:58 GMT
Content-Length: 362
Content-Type: application/xml;charset=UTF-8
Server: Apache-Coyote/1.1

<?xml version="1.0” encoding=”utf-8”?>
 <DeviceCertificateSigningResponse>
        <Version>1.0</Version>
        <Build>1.1.4</Build>
        <TransactionId>12344</TransactionId>
        <Status>FORMAT_ERROR</Status>
        <Error>
          <ErrorCode>FM:123</ErrorCode>
         <ErrorText>An XML format error</ErrorText>
       </Error>
 </DeviceCertificateSigningResponse>
```

Example: Response to Ad Hoc Device Certificate Signing Request – other error

The following message is returned in response to Device CSR when the DCC failed to issue a Device Certificate.

```
HTTP/1.1 200 OK
Date: Tue, 13 May 2014 12:15:58 GMT
Content-Length: 362
Content-Type: application/xml;charset=UTF-8
Server: Apache-Coyote/1.1

<?xml version="1.0” encoding=”utf-8”?>
<DeviceCertificateSigningResponse ID="clientid1">
        <Version>1.0</Version>
        <Build>1.1.4</Build>
        <TransactionId>12345</TransactionId>
        <Status>CSR_ERROR</Status>
        <Error>
          <ErrorCode>CR:9999</ErrorCode>
          <ErrorText>Request for duplicate certificate not permitted</ErrorText>
       </Error>
</DeviceCertificateSigningResponse>
```

Response to Ad Hoc Device Certificate Signing Request: Element Table

Element Name	***Description***
DeviceCertificateSigningResponse	*The root element*
Version	*This element contains the version of the web service interface. In the schema specified in Appendix B of this document, this value is set to "1.0"*
Build	*This element specifies the software build of the web service.*
TransactionId	*This is the SMKI internal reference to the request.*
Status	*This element reports on the condition of the response. See the section "*Response Status*"*
Certificate	*This element contains the 'base64text' field (as defined in RFC 7468 section 3) of a DER X509v3 certificate without whitespace. The element shall NOT contain the 'preeb' and 'posteb' fields.*
Error	*Container for ErrorCode and ErrorText*
ErrorCode	*This element holds an internal reference code to a specific error occurrence. See the section "*Response Status*"*
ErrorText	*This element holds a human readable error string corresponding to the ErrorCode. See the section "*Response Status*"*

Response to Ad Hoc Device Certificate Signing Request: Attribute Table

Attribute Name	***Description***
ID	*This holds the client reference to the original request.*

Response Status

Value	***Error Code***	***Description***
SUCCESS	*n/a*	*This value indicates a certificate has been generated and is returned in the response.*
UNKNOWN_DEVICE	*UD:<Value>*	*The request has been rejected. The device has not had a Device Certificate previously and hence the request to replace an existing certificate is not valid.*
ISSUANCE_ANOMALY	*CA:<Value>*	*The request has been rejected. A certificate issued from the submitted CSR would result in unexpected issuance behaviour. Manual action by the Registration Authority would need to be taken to allow a future submission of this CSR to result in a certificate.*
CSR_ERROR	*CR:<Value>*	*The request has failed. This is due to a corrupt CSR or incorrect CSR format. The client should correct the mistake and re-submit.*
CA_ERROR	*CA:<Value>*	*The request has failed. An internal error has prevented the CA from issuing the certificate. Re-submission may fix this issue.*
FORMAT_ERROR	*FM:<Value>*	*The request has failed. This is due to the request XML format error. The client should correct the mistake and re-submit.*
WORKFLOW_ERROR	*WF:<Value>*	*The request has failed. A workflow error has prevented to issuance of the certificate. Re-submission is unlikely to remedy this issue and should report the error code to the Service Desk.*

Appendix B Schema for Ad Hoc Device CSR Web Service interface

This section specifies the XML schema that will be used to verify the contents for the web service request and response messages relevant to the Ad Hoc Device CSR Web Service interface, as per the figure below.

The Ad Hoc Device CSR Web Service interface version will be specified in the URL, the schema filename and data contained in the XML requests and responses. The web service interface version allowed value will be hardcoded in the schema.

There will be different URL used when the XML schema for the Ad Hoc Device CSR Web Service interface changes.

```
<?xml version="1.0" encoding="UTF-8"?>
<xsd:schema xmlns:xsd="http://www.w3.org/2001/XMLSchema" elementFormDefault="qualified"
attributeFormDefault="unqualified">
  <xsd:element name="DeviceCertificateSigningResponse">
    <xsd:complexType>
      <xsd:sequence>
        <xsd:element name="Version">
            <xsd:simpleType>
            <xsd:restriction base="xsd:string">
              <xsd:enumeration value="1.0"/>
            </xsd:restriction>
          </xsd:simpleType>
        </xsd:element>
        <xsd:element name="Build" type="xsd:string" nillable="false" />
        <xsd:element name="TransactionId" type="xsd:positiveInteger" nillable="false"/>
        <xsd:element name="Status" nillable="false">
          <xsd:simpleType>
            <xsd:restriction base="xsd:string">
              <xsd:enumeration value="SUCCESS"/>
              <xsd:enumeration value="ISSUANCE_ANOMALY"/>
              <xsd:enumeration value="UNKNOWN_DEVICE"/>
              <xsd:enumeration value="CA_ERROR"/>
              <xsd:enumeration value="CSR_ERROR"/>
              <xsd:enumeration value="FORMAT_ERROR"/>
              <xsd:enumeration value="WORKFLOW_ERROR"/>
            </xsd:restriction>
          </xsd:simpleType>
        </xsd:element>
        <xsd:choice>
          <xsd:element name="Certificate" type="xsd:base64Binary" nillable="true"/>
          <xsd:element name="Error">
            <xsd:complexType>
              <xsd:sequence>
                <xsd:element name="ErrorCode" nillable="false">
                  <xsd:simpleType>
                    <xsd:restriction base="xsd:string">
                      <xsd:minLength value="1"/>
                      <xsd:maxLength value="10"/>
                      <xsd:pattern value="[A-Z]{2}:[A-Za-z0-9]+"/>
                    </xsd:restriction>
                  </xsd:simpleType>
                </xsd:element>
                <xsd:element name="ErrorText" type="xsd:string" nillable="false"/>
              </xsd:sequence>
            </xsd:complexType>
          </xsd:element>
```

```
            </xsd:choice>
         </xsd:sequence>
         <xsd:attribute name="ID" use="optional">
            <xsd:simpleType>
               <xsd:restriction base="xsd:string">
                  <xsd:minLength value="1"/>
                  <xsd:maxLength value="32"/>
               </xsd:restriction>
            </xsd:simpleType>
         </xsd:attribute>
      </xsd:complexType>
   </xsd:element>
   <xsd:element name="DeviceCertificateSigningRequest">
      <xsd:complexType>
         <xsd:sequence>
            <xsd:element name="Version">
               <xsd:simpleType>
                  <xsd:restriction base="xsd:string">
                     <xsd:enumeration value="1.0"/>
                  </xsd:restriction>
               </xsd:simpleType>
            </xsd:element>
            <xsd:element name="CertificateSigningRequest" nillable="false">
                   <xsd:simpleType>
                  <xsd:restriction base="xsd:base64Binary"/>
               </xsd:simpleType>
            </xsd:element>
         </xsd:sequence>
         <xsd:attribute name="ID" use="required">
            <xsd:simpleType>
               <xsd:restriction base="xsd:string">
                  <xsd:minLength value="1"/>
                  <xsd:maxLength value="32"/>
               </xsd:restriction>
            </xsd:simpleType>
         </xsd:attribute>
      </xsd:complexType>
   </xsd:element>
</xsd:schema>
```

Appendix C Submission of Batched CSRs via the Batched Device CSR Web Service Interface

In order to submit the Device CSRs that are the subject of a Batched CSR via the Batched Device CSR Web Service interface, a request shall be sent by the requestor to SMKI using HTTP POST.

The batch submission response shall be returned by the DCC, providing the field “BatchId” upon successful submission. The value of “BatchId” shall be used in the retrieval of Device Certificates, as specified in Appendix D of this document.

The destination URL for the post will include the web service interface version and must match the version specified in the section of this Appendix C titled “**Batched CSR Response message: Element Table**” and will take the form as set out below:

a) https://example.com:443/1.0/PortalCSRBatch/SubmitCSRBatch

where “1.0” in the above URL is the web service interface version

Example: Submit Batched CSR Message

The following message is used to request Device Certificates from SMKI via the Batched Device CSR Web Service.

```
Host: localhost:443
Content-Length: 439
User-Agent: Jakarta Commons-HttpClient/3.0.1
Content-Type: application/xml;charset=UTF-8

<?xml version="1.0” encoding=”utf-8”?>
<SubmitCSRBatch ID="b1999">
        <Version>1.0</Version>
        <DeviceCSR ID="ID0">UjBsR09EbGhj………1tQ1p0dU1GUXhEUzhi</DeviceCSR>
        <DeviceCSR ID="ID1">UjBsR09EbGh……..U1GUXhEUzhi</DeviceCSR>
        <DeviceCSR ID="ID2">UjBsR09…..0dU1GUXhEUzhi</DeviceCSR>
</SubmitCSRBatch>
```

Submit Batched CSR Message: Element Table

Element Name	*Description*
SubmitCSRBatch	The root element
Version	This element contains the version of the web service interface. In the schema specified in Appendix E of this document, this value is set to “1.0”
DeviceCSR	This element contains the ‘base64text’ field (as defined in RFC 7468 section 3) of the PKCS#10 certificate signing request (CSR) without whitespace. The element shall NOT contain the ‘preeb’ and ‘posteb’ fields.

Submit Batched CSR Message: Attribute Table

Attribute Name	*Parent Element*	*Description*
ID	SubmitCSR Batch	The client reference to the batch request. This value will be returned in the completed batch result.

ID	DeviceCSR	The client reference to an individual CSR request within the batch request. This value will be returned in the completed batch result to help correlate the resulting certificate with the CSR request. This value MUST be unique within the batch. The format of the ID will be enforced by the associated field type defined in the schema.

Example: Response to Batched CSR – success

The following message is returned in response to the “SubmitCSRBatch” request when the submitted Batched CSR has been accepted.

```
HTTP/1.1 200 OK
Date: Tue, 13 May 2014 12:15:58 GMT
Content-Length: 362
Content-Type: application/xml;charset=UTF-8
Server: Apache-Coyote/1.1

<?xml version="1.0” encoding=”utf-8”?>
<SubmitCSRBatchStatus ID=”b1999”>
            <Version>1.0</Version>
            <Build>2.0.8</Build>
            <BatchStatus>PENDING</BatchStatus>
            <BatchId>1234</BatchId>
</SubmitCSRBatchStatus>
```

Example: Response to Batched CSR – Incorrect XML

The following message is returned in response to an invalidly formed “SubmitCSRBatch” request. In this scenario, DCC is unable to return the client supplied ID field.

```
HTTP/1.1 200 OK
Date: Tue, 13 May 2014 12:15:58 GMT
Content-Length: 362
Content-Type: application/xml;charset=UTF-8
Server: Apache-Coyote/1.1

<?xml version="1.0” encoding=”utf-8”?>
 <SubmitCSRBatchStatus>
            <Version>1.0</Version>
            <Build>2.0.8</Build>
            <BatchStatus>FORMAT_ERROR</BatchStatus>
            <Error>
                        <ErrorCode>FM:AA1</ErrorCode>
                        <ErrorText>Invalid XML in request</ErrorText>
            </Error>
</SubmitCSRBatchStatus>
```

Example: Response to Batched CSR– maximum batch size exceeded

The following message is returned in response to the “SubmitCSRBatch” request when the maximum number of certificate signing requests in the request is exceeded. The maximum batch size is 50,000 CSRs, this figure is detailed in SEC Section L8.2. The maximum batch size stated in SEC Section L8.2 takes precedence should the size differ from that stated in this document.

```
HTTP/1.1 200 OK
Date: Tue, 13 May 2014 12:15:58 GMT
Content-Length: 362
Content-Type: application/xml;charset=UTF-8
Server: Apache-Coyote/1.1

<?xml version="1.0" encoding="UTF-8"?>
<SubmitCSRBatchStatus ID=”b1999”>
        <Version>1.0</Version>
        <Build>2.0.8</Build>
        <BatchStatus>FORMAT_ERROR</BatchStatus>
        <Error>
                <ErrorCode>FM:AA2</ErrorCode>
                <ErrorText>Number of submitted CSRs exceeds maximum volume</ErrorText>
        </Error>
</SubmitCSRBatchStatus>
```

Example: Response to Batched CSR response– other error

The following message is returned in response to the “SubmitCSRBatch” request when SMKI failed to accept the Batched CSR.

```
HTTP/1.1 200 OK
Date: Tue, 13 May 2014 12:15:58 GMT
Content-Length: 362
Content-Type: application/xml;charset=UTF-8
Server: Apache-Coyote/1.1

<?xml version="1.0” encoding=”utf-8”?>
<SubmitCSRBatchStatus ID=”b1999”>
        <Version>1.0</Version>
        <Build>2.0.8</Build>
        <BatchStatus>WORKFLOW_ERROR</BatchStatus>
        <Error>
                <ErrorCode>WF:BB2</ErrorCode>
                <ErrorText>An internal error.</ErrorText>
        </Error>
</SubmitCSRBatchStatus>
```

Batched CSR response message: element table

Element Name	*Description*
SubmitCSRBatchStatus	The root element
Version	This element contains the version of the web service interface. In the schema specified in Appendix E, this value is set to “1.0”
Build	This element specifies the software build of the web service.
BatchId	This is the SMKI internal reference to the batch request. This value should be used to query the CSRBatchResult.
BatchStatus	This element reports on the condition of the response, as set out below.
Error	Container for ErrorCode and ErrorText
ErrorCode	This element holds an internal reference code to a specific error occurrence, as set out below.

Element Name	*Description*
ErrorText	This element holds a human readable error string corresponding to the ErrorCode, as set out below

Batched CSR response message: attribute table

Attribute Name	Parent Element	Description
ID	SubmitCSRBatch Status	The client reference to the batch. This value corresponds to the SubmitCSRBatch ID attribute in the SubmitCSRBatch message.

Batched CSR response message: response status values

Value	*Error Code*	*Description*
PENDING	n/a	The Batched CSR has been uploaded, accepted and is awaiting approval.
FORMAT_ERROR	FM:<Value>	The request has failed. This is due to the request XML format error. The client should correct the mistake and re-submit the request.
WORKFLOW_ERROR	WF:<Value>	The request has failed. A workflow error has prevented acceptance of the batch request. Re-submission is unlikely to remedy this issue and should report the error code to the Service Desk.

Appendix D Retrieval of Device Certificates as a result of Batched CSR submission

In order to retrieve the Device Certificates that are the subject of a Batched CSR submitted via the Batched Device CSR Web Service interface, a batch result poll request shall be sent by the requestor to SMKI using HTTP GET.

The batch result shall be returned by the DCC using the form field “BatchId”, which will be encoded within the GET URL. The value of the “BatchId” field is returned to the requesting system in response to the initial successful “SubmitCSRBatch” web service message. Parties may query for batches they have submitted, however any other values of the “BatchId” field will be rejected.

The destination URL for the get will include the web service interface version and must match the version specified in the section of this Appendix D titled “**Batched CSR Result: Element Table**” and will take the form as set out below:

b) https://example.com:443/1.0/PortalCSRBatch/CSRBatchResult?BatchId=99, where “1.0” in the above URL is the web service interface version

Example: Batched CSR Result Message – Incomplete batch processing

The following message is returned in response to “CSRBatchResult” query and the corresponding batch processing has not been completed. The following batch status values may be returned in this message and where such values are defined in the section titled “Batched CSR Result: BatchStatus values” within this Appendix:

PENDING, REJECTED, PARSING, QUEUED, PROCESSING, PAUSED, TAMPERED

```
HTTP/1.1 200 OK
Date: Tue, 13 May 2014 12:15:58 GMT
Content-Length: 362
Content-Type: application/xml;charset=UTF-8
Server: Apache-Coyote/1.1

<?xml version="1.0" encoding="UTF-8"?>
<CSRBatchResult ID="b1999">
            <Version>1.0</Version>
            <Build>2.0.8</Build>
            <BatchStatus>PENDING</BatchStatus>
            <BatchId>1234</BatchId>
</CSRBatchResult>
```

Example: Batched CSR Result Message – Batch Completed

The following message is returned in response to a “CSRBatchResult” query when each Device CSR has been processed. This file shall contain, for all Device CSRs that were included in the corresponding Batched CSR, either a successfully generated Device Certificate or details of rejected Device CSR.

```
HTTP/1.1 200 OK
Date: Tue, 13 May 2014 12:15:58 GMT
Content-Length: 662
Content-Type: application/xml;charset=UTF-8
Server: Apache-Coyote/1.1

<?xml version="1.0" encoding="UTF-8"?>
<CSRBatchResult ID="b1999">
        <Version>1.0</Version>
        <Build>2.0.8</Build>
        <BatchStatus>COMPLETED</BatchStatus>
        <BatchId>1234</BatchId>
        <DeviceCertificate ID="ID000000">
                <Status>SUCCESS</Status>
                <Certificate>UjBsR09EbGhjZ0dTQUxNQUF………..Q1p0dU1GUXhEUzhi</Certificate>
        </DeviceCertificate>
        <DeviceCertificate ID="ID000001">
                <Status>CSR_ERROR</Status>
               <Error>
                        <ErrorCode>CR:CC1</ErrorCode>
                        <ErrorText>Wrong CSR OID</ErrorText>
                </Error>
        </DeviceCertificate>
        <DeviceCertificate ID="ID000002">
                <Status>SUCCESS</Status>
                <Certificate>UjBsR09EbGhjZ0d………..Q1p0dU1GUXhEUzhi</Certificate>
        </DeviceCertificate>
</CSRBatchResult>
```

Example: Batched CSR Result Message – Unknown BatchId

The following message is returned in response to a "CSRBatchResult" query where the supplied "BatchId" does not exist.

```
HTTP/1.1 200 OK
Date: Tue, 13 May 2014 12:15:58 GMT
Content-Length: 362
Content-Type: application/xml;charset=UTF-8
Server: Apache-Coyote/1.1

<?xml version="1.0" encoding="UTF-8"?>
<CSRBatchResult>
        <Version>1.0</Version>
        <Build>2.0.8</Build>
        <BatchStatus>FORMAT_ERROR</BatchStatus>
        <Error>
                <ErrorCode>FM:AA3</ErrorCode>
                <ErrorText>Unknown BatchId</ErrorText>
        </Error>
</CSRBatchResult>
```

Example: Batched CSR Result Message – Other Error

The following message is returned in response to a "CSRBatchResult" query when SMKI failed to interrogate the batch state.

```
HTTP/1.1 200 OK
Date: Tue, 13 May 2014 12:15:58 GMT
Content-Length: 362
Content-Type: application/xml;charset=UTF-8
Server: Apache-Coyote/1.1

<?xml version="1.0" encoding="UTF-8"?>
<CSRBatchResult>
        <Version>1.0</Version>
        <Build>2.0.8</Build>
        <BatchStatus>WORKFLOW_ERROR</BatchStatus>
        <Error>
                <ErrorCode>WF:BB1</ErrorCode>
                <ErrorText>An Internal Error</ErrorText>
        </Error>
</CSRBatchResult>
```

This element contains the 'base64text' field (as defined in RFC7468 section 3) of a DER X509v3 certificate without whitespace. The element shall NOT contain the 'preeb' and 'posteb' fields.

Batched CSR Result: Element Table

Element Name	Description
CSRBatchResult	The root element
Version	This element contains the version of the web service interface. In the schema specified in Appendix E, this value is set to "1.0"
Build	This element specifies the software build of the web service.
BatchId	This is the SMKI internal reference to the batch request.
BatchStatus	This element reports on the condition of the response. See the section "Batched CSR Result: BatchStatus values"
Error	Container for ErrorCode and ErrorText
ErrorCode	This element holds an internal reference code to a specific error occurrence. See the section "Response Status" and "Batched CSR Result: Status values".
ErrorText	This element holds a human readable error string corresponding to the ErrorCode.
DeviceCertificate	This element holds a response to a Certificate Signing Request.
Certificate	This element contains the 'base64text' field (as defined in RFC 7648 section 3) of a DER X509v3 certificate without whitespace. The element shall NOT contain the 'preeb' and 'posteb' fields.
Status	This element holds the outcome of processing the Certificate Signing Request. See the section "Batched CSR Result: Status values"

Batched CSR Result: Attribute Table

Attribute Name	Parent Element	Description
ID	CSRBatchResult	The client reference to the batch. This value corresponds to the SubmitCSRBatch ID attribute in the SubmitCSRBatch message.
ID	DeviceCertificate	The client reference to an individual certificate within the batch response. This value corresponds to the DeviceCSR ID attribute in the SubmitCSRBatch message

Batched CSR Result: BatchStatus values

Value	Error Code	Description
PENDING	n/a	The batch has been uploaded, accepted and is awaiting approval.
REJECTED	n/a	The batch has been rejected by the Registration Authority. The batch will not be processed further.
PARSING	n/a	The batch has been approved by the Registration Authority and the batch request and associated Certificate Signing Requests are being parsed
QUEUED	n/a	The batch request and associated Certificate Signing Requests have been parsed and are queued ready for processing.
PROCESSING	n/a	The batch request and associated Certificate Signing Requests are being processed.
PAUSED	n/a	The daily time window for processing batches is closed. The processing of the batch is suspended until the next processing time window.
COMPLETED	n/a	The processing of the batch is completed. The results of the batch processing are contained with the returned XML.
TAMPERED	n/a	The submitted batch contents has changed between upload and parsing. The batch will not be processed further.
FORMAT_ERROR	FM:<Value>	The query for the batch result has failed. This is due to the request format error. The client should correct the mistake and re-submit the request.
WORKFLOW_ERROR	WF:<Value>	The query for the batch result has failed. A workflow error has prevented construction of the batch result message. Re-submission is unlikely to remedy this issue. This issue should be reported, stating the error code, to the DCC helpdesk.

Batched CSR Result: Status values

Value	Error Code	Description
SUCCESS	n/a	This value indicates a Certificate has been generated and is returned in the response.
ISSUANCE_ANOMALY	CA:<Value>	The request has been rejected. A certificate issued from the submitted CSR would result in unexpected issuance behaviour. Manual action by the Registration Authority team would need to be taken to allow a future submission of this CSR to result in a certificate.
INELIGIBLE	IN:<Value>	This value indicates that the CSR has failed the eligibility check as set out in Section L3.16 of the Code. The Remote Party Role of the requester is limited to requesting certificates for meters in certain provisioning states. The Error Code will detail the reason that the eligibility check failed.
CSR_ERROR	CR:<Value>	The request has failed. This is due to a corrupt CSR or incorrect CSR format. The client should correct the mistake and re-submit the CSR.
CA_ERROR	CA:<Value>	The request has failed. An internal error has prevented the CA from issuing the certificate. Re-submission of the CSR may fix this issue.
WORKFLOW_ERROR	WF:<Value>	The request has failed. A workflow error has prevented issuance of the certificate. Re-submission is unlikely to remedy this issue. This issue should be reported, stating the error code, to the Service Desk.

Appendix E Schema for Batched Device CSR Web Service interface

```
<?xml version="1.0" encoding="UTF-8"?>
<xs:schema xmlns:xs="http://www.w3.org/2001/XMLSchema" elementFormDefault="qualified"
attributeFormDefault="unqualified">
  <xs:element name="SubmitCSRBatch" nillable="false">
    <xs:complexType>
      <xs:sequence>
        <xs:element ref="Version"/>
        <xs:sequence maxOccurs="unbounded">
          <xs:element name="DeviceCSR" nillable="false">
            <xs:complexType>
              <xs:simpleContent>
                <xs:extension base="xs:base64Binary">
                  <xs:attribute name="ID" use="required">
                    <xs:simpleType>
                      <xs:restriction base="xs:ID">
                        <xs:minLength value="1"/>
                        <xs:maxLength value="100"/>
                      </xs:restriction>
                    </xs:simpleType>
                  </xs:attribute>
                </xs:extension>
              </xs:simpleContent>
            </xs:complexType>
          </xs:element>
        </xs:sequence>
      </xs:sequence>
      <xs:attribute name="ID" use="required">
        <xs:simpleType>
          <xs:restriction base="xs:string">
            <xs:minLength value="1"/>
            <xs:maxLength value="256"/>
          </xs:restriction>
        </xs:simpleType>
      </xs:attribute>
    </xs:complexType>
  </xs:element>
  <xs:element name="SubmitCSRBatchStatus" nillable="false">
    <xs:complexType>
      <xs:sequence>
        <xs:element ref="Version"/>
        <xs:element ref="Build"/>
        <xs:element name="BatchStatus" nillable="false">
          <xs:simpleType>
            <xs:restriction base="xs:string">
              <xs:enumeration value="PENDING"/>
              <xs:enumeration value="FORMAT_ERROR"/>
              <xs:enumeration value="WORKFLOW_ERROR"/>
            </xs:restriction>
          </xs:simpleType>
        </xs:element>
        <xs:choice>
          <xs:element ref="BatchId"/>
          <xs:element ref="Error"/>
        </xs:choice>
      </xs:sequence>
      <xs:attribute name="ID" use="optional">
        <xs:simpleType>
          <xs:restriction base="xs:string">
            <xs:minLength value="1"/>
            <xs:maxLength value="256"/>
          </xs:restriction>
        </xs:simpleType>
      </xs:attribute>
    </xs:complexType>
  </xs:element>
  <xs:element name="CSRBatchResult">
    <xs:complexType>
      <xs:sequence>
        <xs:element ref="Version"/>
        <xs:element ref="Build"/>
        <xs:element name="BatchStatus" nillable="false">
          <xs:simpleType>
            <xs:restriction base="xs:string">
              <xs:enumeration value="PENDING"/>
              <xs:enumeration value="REJECTED"/>
              <xs:enumeration value="PARSING"/>
              <xs:enumeration value="QUEUED"/>
              <xs:enumeration value="PROCESSING"/>
              <xs:enumeration value="PAUSED"/>
              <xs:enumeration value="COMPLETED"/>
              <xs:enumeration value="TAMPERED"/>
              <xs:enumeration value="FORMAT_ERROR"/>
              <xs:enumeration value="WORKFLOW_ERROR"/>
            </xs:restriction>
          </xs:simpleType>
        </xs:element>
        <xs:choice minOccurs="0">
          <xs:element ref="Error"/>
          <xs:sequence>
            <xs:element ref="BatchId"/>
            <xs:sequence minOccurs="0" maxOccurs="unbounded">
              <xs:element name="DeviceCertificate">
                <xs:complexType>
                  <xs:sequence>
                    <xs:element name="Status" nillable="false">
                      <xs:simpleType>
                        <xs:restriction base="xs:string">
                          <xs:enumeration value="SUCCESS"/>
                          <xs:enumeration value="ISSUANCE_ANOMALY"/>
                          <xs:enumeration value="INELIGIBLE"/>
                          <xs:enumeration value="CSR_ERROR"/>
                          <xs:enumeration value="CA_ERROR"/>
                          <xs:enumeration value="WORKFLOW_ERROR"/>
                        </xs:restriction>
                      </xs:simpleType>
                    </xs:element>
                    <xs:choice>
                      <xs:element name="Certificate" type="xs:base64Binary" nillable="false"/>
                      <xs:element ref="Error"/>
                    </xs:choice>
                  </xs:sequence>
                  <xs:attribute name="ID" use="required">
                    <xs:simpleType>
                      <xs:restriction base="xs:ID">
                        <xs:minLength value="1"/>
                        <xs:maxLength value="100"/>
                      </xs:restriction>
                    </xs:simpleType>
                  </xs:attribute>
```

```
                        </xs:complexType>
                     </xs:element>
                  </xs:sequence>
               </xs:sequence>
            </xs:choice>
         </xs:sequence>
         <xs:attribute name="ID">
            <xs:simpleType>
               <xs:restriction base="xs:string">
                  <xs:minLength value="1"/>
                  <xs:maxLength value="256"/>
               </xs:restriction>
            </xs:simpleType>
         </xs:attribute>
      </xs:complexType>
   </xs:element>
   <xs:element name="Version" nillable="false">
      <xs:simpleType>
         <xs:restriction base="xs:string">
            <xs:enumeration value="1.0"/>
         </xs:restriction>
      </xs:simpleType>
   </xs:element>
   <xs:element name="Build" type="xs:string" nillable="false"/>
   <xs:element name="BatchId" type="xs:positiveInteger" nillable="false"/>
   <xs:element name="Error" nillable="false">
      <xs:complexType>
         <xs:sequence>
            <xs:element name="ErrorCode" nillable="false">
               <xs:simpleType>
                  <xs:restriction base="xs:string">
                     <xs:minLength value="1"/>
                     <xs:maxLength value="10"/>
                     <xs:pattern value="[A-Z]{2}:[A-Za-z0-9]+"/>
                  </xs:restriction>
               </xs:simpleType>
            </xs:element>
            <xs:element name="ErrorText" type="xs:string" nillable="false"/>
         </xs:sequence>
      </xs:complexType>
   </xs:element>
</xs:schema>
```

Appendix F Certificate Signing Request Structure

Information to be contained within an Organisation CSR

Section	Attributes	Value
Version		Version 0
Subject	Common Name (id-at-commonName)	This field shall only be populated where, should it be placed in an Organisation Certificate produced using this CSR's details, it would comply with the requirements for the Subject X520 Common Name field in such Organisation Certificates, where those terms have their Appendix B Organisation Certificate Policy meaning.
	Organisational Unit (id-at-organizationalUnitName)	Remote Party Role Code of the Subject of the Certificate (2 character hexadecimal representation of the Remote Party Role Code). E.g. for supplier, value = '02'
	Subject Unique Identifier (id-at-uniqueIdentifier)	The 64 bit EUI-64 Compliant identifier of the subject of the Certificate
Subject Public Key Information	Public Key Algorithm	id-ecPublicKey
	Prime256r1 (256 bit)	Public Key Value
Key Usage	Criticality	True
	Key Usage	digitalSignature or keyAgreement
Signature Algorithm		ecdsa-with-SHA256

CSR forms submitted to the SMKI Portal via DCC Gateway Connection and the SMKI Portal via the Internet will be accepted in PKCS#10 format Base64 encoded. The standard format for CSR forms submitted to the SMKI Portal via DCC Gateway Connection and the SMKI Portal via the Internet will be ASN.1 DER, including either styles of PEM header (i.e. -----BEGIN CERTIFICATE REQUEST----- and -----END CERTIFICATE REQUEST----- or -----BEGIN NEW CERTIFICATE REQUEST----- and -----END NEW CERTIFICATE REQUEST-----). The following variants for CSR forms submitted to the SMKI Portal via DCC Gateway Connection or SMKI Portal via the Internet will also be accepted:

a) No PEM headers

b) Base64 all in one line

c) Base64 with line breaks at 64 or 76 characters

d) If line breaks are used the \n and \r\n are both acceptable

Information to be contained within a Device CSR

Section	Attributes				Value
Version					Version 0
Subject					Empty
Subject Public Key Information	Public Key Algorithm				id-ecPublicKey
	Prime256r1 (256 bit)				Public Key Data
Key Usage	Criticality				True
	Key Usage				digitalSignature or keyAgreement
Subject Alternative Name	General Name	Other Name	id-on-hardwareModuleName	hwType	Object Identifier, OID
				hwSerialNum	Device ID (EUI-64)
Signature Algorithm					ecdsa-with-SHA256

CSR forms submitted to the SMKI Portal via DCC Gateway Connection will be accepted in PKCS#10 format Base64 encoded. The standard format for CSR forms submitted to the SMKI Portal via DCC Gateway Connection will be ASN.1 DER, including either styles of PEM header (i.e. -----BEGIN CERTIFICATE REQUEST----- and -----END CERTIFICATE REQUEST----- or -----BEGIN NEW CERTIFICATE REQUEST----- and -----END NEW CERTIFICATE REQUEST-----). The following variants for Device CSRs submitted to the SMKI Portal via DCC Gateway Connection will also be accepted:

a) No PEM headers

b) Base64 all in one line

c) Base64 with line breaks at 64 or 76 characters

d) If line breaks are used the \n and \r\n are both acceptable

CSRs submitted via the Ad Hoc Device CSR Web Service interface or the Batched Device CSR Web Service interface shall not use PEM headers, as set out in Appendix A and Appendix C respectively.

Format of Batched Certificate Signing Requests via SMKI Portal interface

The format that shall be used for .zip files is defined in *info-zip.org/doc/appnote-19970311-iz.zip.*

Request File

a) The format of the batch request is a ZIP archive containing up to 50,000 individual files with a "csr" extension, which must be in the following format:

b) Each of these files must be uniquely named in the root level of the archive;

c) The individual files must contain a Base64 (as defined by RFC 7468 Section 3) encoded PKCS#10 CSR; and

d) The name of the each file with a 'csr' extension within the ZIP archive is preserved within the SMKI workflow, excluding the "csr" extension, so that the name of the corresponding Device Certificate file in the response ZIP archive will include the name supplied in the 'csr' file.

Response File

The "Response File" is a ZIP archive containing:

a) a text file record for each CSR contained within the Batched CSR, which shall contain the fields as set out immediately below:

   i. identifier for the CSR contained within the Batched CSR;

   ii. the file name for the CSR;

   iii. the status of the processing of the CSR, which shall have a value of one of 'success', 'error', 'anomaly' or 'ineligible'; and

   iv. where relevant, an error code associated with the processing of the CSR; and

b) a ZIP archive which contains all Certificates from the request which have been issued, in the following format:

   i. Certificates will be in Base64 encoded X.509 format;

   ii. The filename is that of the request ZIP file with "-response" appended, and issued certificates are stored in the root level of the archive; and

   iii. The Certificate names are the same as their corresponding request files, but with the "crt" rather than "csr" extension.

Appendix G Authentication Credentials

The SMKI Portal for Users, Ad-Hoc Device CSR Web Service interface and Batched Device CSR Web Service interface shall use server and client certificates with the following cryptographic properties:

Criteria	*Version*
Protocol	*TLS**
Protocol Cyphers	*ECDHE-RSA-AES256-GCM-SHA384*
	ECDHE-RSA-AES256-SHA384
	ECDHE-RSA-AES128-GCM-SHA256
	ECDHE-RSA-AES128-SHA256
Client Certificate Key	*RSA 2048 bit*
Client Certificate Hash Algorithm	*SHA256*
Server Certificate Key	*RSA 2048 bit*
Server Certificate Hash Algorithm	*SHA256*

* TLS should be implemented in accordance with Java and Apache standards and the SMKI PMA and SSC Guidance (Standards, Procedures and Guidelines) published on the SEC website. The TLS version is specified in the HTTP client protocol initialisation. To enable AES256, the Java runtime should be patched with “JCE Unlimited Strength Jurisdiction Policy Files” for the version of Java being used. This is obtained from the public Oracle Java download web pages.

Information to be contained within a CSR for IKI Certificates (client credentials) used to access the Ad Hoc Device CSR Web Service interface and/or the Batched Device CSR Web Service interface

Each CSR for an IKI Certificate used to access the Ad Hoc Device CSR Web Service interface and/or the Batched Device CSR Web Service interface shall comply with the format as set out immediately below. Each such CSR shall only apply to one of the interfaces listed immediately below:

a) Ad Hoc Device CSR Web Service interface; or

b) Batched Device CSR Web Service interface.

Section	**Attributes**	**Value**
Version		Version 0
Subject	Organisation (id-at-organizationName)	Organisation Trading Name
	Organisational Unit (id-at-organizationalUnitName)	Remote Party Role Code

Section	Attributes	Value
	Common Name (id-at-commonName)	Unique Name of the Authorised System, which the submitting Party must ensure is unique for: 1) multiple CSRs for the Ad Hoc Device CSR Web Service interface; or 2) multiple CSRs for the Batched Device CSR Web Service interface.
Subject Public Key Information	Public Key Algorithm	RSAPublicKey
	Key Size	2048
Key Usage	Criticality	True
	Key Usage	digitalSignature
Signature Algorithm		SHA256withRSAEncryption

Appendix H Definitions

Term	Meaning as defined in SEC
Ad Hoc Device CSR Web Service	Has the meaning given to that expression in the SMKI RAPP.
Authorised Responsible Officer	Has the meaning given to that expression in the SMKI RAPP.
AES	Advanced Encryption Standard
Batched Device CSR Web Service	Has the meaning given to that expression in the SMKI RAPP.
Device CSR	Means a CSR submitted in respect of a Device Certificate.
IKI Certification Authority	Has the meaning given to that expression in the IKI Certificate Policy.
Issue	Has the meaning given to that expression in SEC Section A and like terms shall be interpreted accordingly.
Organisation CSR	Means a CSR submitted in respect of an Organisation Certificate.
Portal	Portal is a generic term in the SMKI SEC Documents. It refers to a web-based interface, within which there may be multiple views, depending on the permissions of the individual accessing it.
SMKI Portal	‘Portal’ is a generic term in the SMKI environment: the portals for the OCA and DCA exist as separate URLs within the primary SMKI Portal with security applied in line with the ARO’s role.
SMKI User Guide	Means a user guide for the SMKI Services produced and maintained by the DCC.

Version: N3.0

Appendix N

SMKI Code of Connection

Purpose and Scope

This document is the SMKI Code of Connection produced pursuant to Section L4.5 of the Code.

For the purpose of the SMKI Code of Connection, defined terms shall have the meaning in SEC Section A (Definitions and Interpretation), SEC Appendix M (SMKI Interface Design Specification) and Appendix A of this document.

1. Connection Mechanism

The DCC shall ensure that only persons who are Authorised Responsible Officers (AROs) and have been issued with the appropriate IKI credentials used to access SMKI Services, as defined in the SMKI RAPP, shall be able to access the SMKI Services on behalf of their organisation. Prior to use any of the SMKI Interfaces, any person representing a Party or RDP shall first become an Authorised Responsible Officer, via the process as set out in the SMKI RAPP.

Any Party or RDP which has use of a DCC Gateway Connection may connect to the SMKI Services via that DCC Gateway Connection, and shall use this mechanism to connect to the service unless it is not reasonably practicable to do so. Any Party or RDP may connect to the SMKI Services via an Internet connection where such Party or RDP does not have a DCC Gateway Connection or where it is not reasonably practicable to use such a connection.

1.1. Browser Policy

The DCC shall publish and keep up to date the web browsers and versions which the SMKI Portal interface via a DCC Gateway Connection, and SMKI Portal interface via the Internet supports.

The DCC shall not be required to continue to support any browser versions from which the browser's vendor removes support.

Browsers other than those published may also be compatible, though they will not be supported.

The DCC shall ensure that the SMKI Portal interface via a DCC Gateway Connection and SMKI Portal interface via the Internet are tested with the published browsers on different operating systems. The DCC shall publish and keep up to date the list of operating systems that have been tested.

Operating systems other than those listed above may also be compatible, though they will not be supported.

The browsers (and versions) and operating systems supported by the DCC shall be reviewed from time to time. The DCC shall seek views from Parties and RDPs prior to the withdrawal of support for any version of a browser, a browser itself, or an operating system set out above.

2. SMKI Services interfaces

The DCC shall ensure that SMKI Services shall be made available via four interfaces, as set out in this document. The DCC shall provide relevant technical support information to persons in respect of the use of the SMKI interfaces, upon receipt of a request via the Service Desk.

2.1. SMKI Services interfaces via a DCC Gateway Connection

2.1.1 SMKI Portal interface via a DCC Gateway Connection

The DCC shall at all times (subject to Planned Maintenance) provide and maintain an interface where a Party or RDP may connect to the SMKI Portal interface using a compatible web browser via a DCC Gateway Connection.

The DCC shall ensure that the SMKI Portal interface via a DCC Gateway Connection enables Parties or RDPs with access to the interface to navigate to a landing page via a published URL and from there, further choose to:

(a) submit Organisation Certificate Signing Requests (CSR) and retrieve resulting Organisation Certificates;

(b) submit Ad Hoc Device CSRs and retrieve resulting Device Certificates; and

(c) submit Batched CSRs and retrieve resulting Device Certificates.

2.1.2 Ad Hoc Device CSR Web Service interface

The DCC shall at all times (subject to Planned Maintenance) provide and maintain an Ad Hoc Device CSR Web Service interface to which an Authorised Subscriber for Device Certificates, which is one of the DCC, Import Supplier, or Gas Supplier, may connect.

The DCC shall ensure that the Ad Hoc Device CSR Web Service interface supports submission of Ad Hoc Device CSRs to the DCC and the subsequent issuance of Device Certificates by the DCC, to support the replacement of a certificate on a Device.

2.1.3 Batched Device CSR Web Service interface

The DCC shall at all times (subject to Planned Maintenance) provide and maintain a Batched Device CSR Web Service interface to which an Authorised Subscriber for Device Certificates may connect.

The DCC shall ensure that the Batched Device CSR Web Service interface supports submission of Batched CSRs to the DCC and the subsequent issuance of Device Certificates by the DCC.

2.2. SMKI Portal interface via the Internet

The DCC shall at all times (subject to Planned Maintenance) provide and maintain an interface where a Party or RDP may connect to the SMKI Portal interface via the Internet using a compatible web browser.

The DCC shall enable Parties or RDPs with access to the SMKI Portal interface via the Internet to:

(a) submit Organisation CSRs and retrieve resulting Organisation Certificates.

2.3. Authentication to SMKI Services interfaces

2.3.1 Authentication to SMKI Portal interface via a DCC Gateway Connection or via the Internet

The DCC shall secure the SMKI Portal interface via a DCC Gateway Connection or SMKI Portal interface via the Internet through a mutually authenticated TLS session as set out in the SMKI Interface Design Specification.

The DCC shall publish to Parties and RDPs a 'SMKI User Guide' meeting the requirements of this document.

In order to authenticate to the SMKI Portal, Cryptographic Credential Tokens shall be issued in accordance with the procedures set out in the SMKI RAPP.

Each Party or RDP wishing to access the SMKI Portal interface shall install the Authentication Client software on each ARO's computer used to access the SMKI Portal interface.

The DCC shall make the Authentication Client software available to Parties and RDPs and ensure that the software:

(a) is accessible via a URL that shall be specified and updated from time to time in the SMKI User Guide, using One Way Authentication which can be validated using a 'CA Browser Forum 'server certificate that is signed by a 'Root CA' that is present in in the Windows 'Trusted Root Certification Authorities' certificate store';

(b) is compatible with published operating systems;

(c) is digitally signed using the private key associated with a code signing certificate that is signed by a root CA that is present in in the Windows 'Trusted Root Certification Authorities' certificate store'; and

(d) is supported by instructions as to how to install the Authentication Client software, as set out in the SMKI User Guide.

The Party or RDP may download, and verify the authenticity and integrity of, the Authentication Client software on first use by checking the digital signature used to sign the software and validating the 'CA Browser Forum'[1] server certificate using the certification authority certificates present in the Windows 'Trusted Root Certification Authorities' certificate store'. If such checks are successful, the Party or RDP may install the Authentication Client software on each computer that they wish to use to access the SMKI Portal. In Windows, "Administrator" privileges are required to install the Authentication Client software but are not required to run such software.

The DCC shall ensure that each Cryptographic Credential Token issued contains the appropriate IKI Certificate and Private Key for that Party or RDP, which is needed to authenticate the ARO to the SMKI Portal interface via the DCC Gateway Connection or the SMKI Portal via the Internet.

Furthermore, the DCC shall ensure that:

(a) access to the Cryptographic Credential Token is PIN-protected and the Private Key corresponding with the IKI Certificate used for authentication cannot be removed from the Cryptographic Credential Token;

(b) the Authentication Client software is made available for use by AROs to enable authentication to the SMKI Portal in conjunction with the Cryptographic Credential Token;

(c) it provides support for the Authentication Client software via the Service Desk;

(d) updates are made available to the Authentication Client software accessible via a URL, as set out in the SMKI User Guide; and

[1] https://cabforum.org/

(e) ensure that all browsers listed in section 1.1 of this document are capable of supporting the requirements set out in this section.

The process for TLS1.2 mutual authentication to the SMKI Portal interface via the DCC Gateway Connection or the SMKI Portal via the Internet is as set out in the SMKI Interface Design Specification.

2.3.2 Authentication to Ad Hoc Device CSR Web Service interface

The DCC shall secure the Ad Hoc Device CSR Web Service interface through a TLS1.2 mutual authenticated session to the SMKI Portal in accordance with the SMKI Interface Design Specification.

Parties require an appropriate IKI Certificate, in order to authenticate to the Ad Hoc Device CSR Web Service interface. This IKI Certificate shall be issued by the DCC on successful completion of the process as set out in the SMKI RAPP and in accordance with the SMKI Interface Design Specification.

2.3.3 Authentication to Batched Device CSR Web Service interface

The DCC shall secure the Batched Device CSR Web Service interface through a TLS1.2 mutually authenticated session to the SMKI Portal as set out in the SMKI Interface Design Specification.

Parties require an appropriate IKI Certificate in order to authenticate to the Batched Device CSR Web Service interface. This shall be issued by DCC on successful completion of the process as set out in the SMKI RAPP in accordance with the SMKI Interface Design Specification.

3. Managing Demand

3.1. Capacity Management

3.1.1 SMKI Portal via a DCC Gateway Connection and SMKI Portal via the Internet

Organisation CSRs

The Registration Authority shall process Organisation Certificate Signing Requests received via the DCC Gateway Connection or via the Internet in the same manner.

Batched CSRs

The Registration Authority shall process Batched CSRs received via either SMKI Portal interface in the same manner.

Batch CSRs are processed overnight, and the system is scaled to process a total, across all Authorised Subscribers, of 375,000 CSRs contained within Batched CSRs from 20:00 to 08:00 each day.

The DCC shall ensure that Batched CSRs submitted before 8:00pm are processed by 8:00am the following day. Batched CSRs received after 8:00pm may be delayed until the following night’s processing period.

In order to preserve the overall system capacity, should a Party foresee a need to submit in excess of 50,000 Device Certificate Signing Requests through the SMKI Portal interface in any 24 hour period, the Party shall take reasonable steps to inform the DCC of the potential additional load at least seven days in advance via the Service Desk. The Batched CSRs exceeding this number shall be queued for processing as soon as reasonably practicable.

Batched CSRs shall be processed by the Registration Authority in turn.

Ad Hoc Device CSRs

The Registration Authority shall process Ad Hoc Device CSRs received via the DCC Gateway Connection.

Each Party shall take reasonable steps not to submit more than 150 Ad Hoc Device CSRs in any 24 hour period without the prior agreement of DCC. Should a Party foresee a need to exceed this number the Party shall take reasonable steps to inform the DCC of the potential additional load at least seven days in advance via the DCC's Service Desk.

3.1.2 Ad Hoc Device CSR Web Service interface

Each Party shall take reasonable steps not to submit more than one Certificate Signing Request via the Ad Hoc Device CSR Web Service interface in any 0.8 second period during core service hours (07:00 to 20:00) and one Certificate Signing Request in any four second period outside of these hours.

Should a Party foresee a need to exceed either of these numbers, the Party shall take reasonable steps to inform the DCC of the potential additional load at least seven days in advance via the Service Desk.

3.1.3 Batched Device CSR Web Service interface

Each Party shall ensure that a synchronous response to the submission of a Batched CSR is received before an additional Batched CSR is submitted via the Batched CSR Web Service interface. Each Party may submit multiple Batched CSRs during the period of time between submission of a Batched CSR and downloading the response file containing the Device Certificates and success/error messages.

Each Party shall comply with the following restrictions in respect of retrieving such Device Certificates:

(a) where a Batched CSR is submitted before 20:00, the Party shall comply with the following restrictions in respect of accessing the response file corresponding with a particular Batched CSR:

i. the Party shall not seek to access the response file containing the Device Certificates prior to 08:00 on the day following the date of submission of the corresponding Batched CSR;

ii. the Party shall not seek to access the response file again via the Batched CSR Web Service interface, at any point once the response file has been successfully retrieved; and

iii. if the response indicates that the Batched CSR has been accepted and that the batch processing is not complete, the Party shall not seek to access the response file more than once each hour during the period from 22:00 and 08:00 on the following day.

(b) where a Batched CSR is submitted after 20:00, the Party shall comply with the following restrictions in respect of accessing the response file corresponding with a particular Batched CSR:

i. the Party shall not seek to access the response file containing the Device Certificates prior to 22:00 on the day after the submission of the corresponding Batched CSR; and

ii. the Party shall not seek to access the response file again via the Batched CSR Web Service interface, at any point once the response file has been successfully retrieved; and

iii. if the response indicates that the Batched CSR has been accepted and that the batch processing is not complete, the Party shall not seek to access the response file again more than once each hour during the period from 22:00 on the day after the submission of the corresponding Batched CSR and 08:00, two days after the date of submission of the corresponding Batched CSR.

Appendix A Definitions

Term	Meaning as defined in SEC
Ad Hoc Device CSR	Means a CSR submitted via the Ad Hoc Device CSR Web Service interface
Authentication Client	Means client software which supports authentication of Authorised Responsible Officers
Batched CSR	Means a Batched Certificate Signing Request with its SEC Section A definition.
One Way Authentication	Means the industry standard terminology for HTTPS whereby the client is not required to authenticate with a client credential
SMKI User Guide	Means the document published by the DCC pursuant to the requirement in section 2.3.1

Version: 7.0

APPENDIX O

SMKI Repository Interface Design Specification

Contents

1 Introduction

1.1 Purpose and Scope

The SMKI Repository Interface Design Specification is a document required by Section L6.4 of the SEC, in order to:

a) specify the technical details of the SMKI Repository Interface; and

b) set out the protocols and technical standards that apply to the SMKI Repository Interface.

1.2 Target Response Times

For the purposes of supporting the measurement of Target Response Times in accordance with Sections L8.4 and L8.5 of the SEC, the terms “sending” and “receipt” should be interpreted as follows:

a) “receipt” means, in relation to a request submitted over a DCC Gateway Connection to obtain any document lodged in the SMKI Repository, the successful completion by DCC of the validation checks in relation to such a request, as set out in the SMKI Repository Interface Design Specification; and

b) “sending” means, in relation to a document lodged in the SMKI Repository, the making available of an electronic copy of that document by the DCC Systems such that it is immediately available to be retrieved over a DCC Gateway Connection via the SMKI Repository Interface.

For the purposes of requests issued other than by a DCC Gateway Connection, the terms “sending” and “receipt” should be interpreted in accordance with the meaning as set out in section 1.2 of the SMKI Interface Design Specification.

2 Interface Definition

The DCC shall make three interfaces, collectively referred to as the SMKI Repository Interface, available via a DCC Gateway Connection through which Parties, RDPs, the SMKI PMA and the Panel (or the Code Administrator acting on their behalf) may access the SMKI Repository:

a) a SMKI Repository Portal interface accessed via a web browser (as set out in section 2.1 of this document);

b) a SMKI Repository Web Service interface that can be accessed by a Party's or an RDP's systems (as set out in section 2.2, Annex A and Annex B of this document); and

c) a SSH File Transfer Protocol Interface (the "SFTP Interface") via an SFTP client (as set out in section 2.3 of this document).

Any DCC Gateway Connection user wishing to manage its credentials used to access the SMKI Repository Web Service interface or SFTP Interface shall ensure that it has access to the SMKI Repository Portal interface, which allows management of such credentials.

The means by which Parties, RDPs, the SMKI PMA, and the Panel (or the Code Administrator acting on their behalf) may access SMKI Repository content without a DCC Gateway Connection, are set out in section 2.6 of the SMKI Interface Design Specification.

The SMKI Code of Connection sets out the methods by which such persons may, communicate over the SMKI Repository Interface, and the methods by which connections to the SMKI Repository interfaces are authenticated and communications taking place over them are secured.

The DCC shall ensure that the SMKI Repository Interface is available in line with Section L6.2 of the Code and shall notify Parties and RDPs in advance of any planned outages of the SMKI Repository Interface. The DCC shall ensure that failover between the live and disaster recovery (DR) environments will be achieved using dynamic routing and network address translation on the DCC Gateway Connection. The SMKI Repository interfaces will be accessed via the same Uniform Resource Locator (URL) in the event of a DR invocation; the traffic for this URL will be routed to the DR site and presented to the DR servers completely transparently to the user.

2.1 SMKI Repository Portal Interface via DCC Gateway Connection

2.1.1 General Obligations

The DCC shall ensure that the SMKI Repository Portal interface enables DCC Gateway Connection users to access the SMKI Repository Portal for the purposes:

a) of viewing, querying and / or obtaining a copy of those documents lodged in the SMKI Repository as set out in section 2.1.3 of this document; and

b) of updating password and user profile details in respect of authentication to the SMKI Repository Portal interface.

The DCC shall publish and make available to Parties, RDPs, the SMKI PMA, and the Panel a SMKI Repository User Guide meeting the requirements for that guide laid out in this document and in the SMKI Repository Code of Connection.

The DCC shall ensure that the SMKI Repository Portal interface available via a DCC Gateway Connection:

a) uses the HTTPS protocol, secured by TLS in line with the protocols set out in Annex C of this document;

b) is accessed via URLs that are set out in the SMKI Repository User Guide;

c) uses Javascript, Cascading Style Sheets (CSS) and images;

d) is compliant with the W3C Web Content Accessibility Guidelines (v2) at "AA" level; and

e) is only accessible using a DCC Gateway Connection.

The process for obtaining a DCC Gateway Connection is detailed in Section H3 of the Code.

The DCC shall ensure that all Organisation Certificates, OCA Certificates, Device Certificates, DCA Certificates, Organisation CRLs and Organisation ARLs lodged in the SMKI Repository are in Base64 DER format. Organisation CRL and Organisation ARL validity is as set out in Annex B to the Code.

2.1.2 Establishing connection to the SMKI Repository Portal interface via a DCC Gateway Connection

In order to establish a connection to the SMKI Repository Portal interface, a DCC Gateway Connection user shall:

a) ensure that their browsers have Javascript enabled;

b) verify the 'CA/Browser Forum' server certificate presented by the SMKI Repository Portal, as described below and, if successfully verified by the browser, accept the certificate;

c) enter a username and password that has been issued for the purpose of authenticating the user to the SMKI Repository Portal interface; and

d) establish a TLS session.

The DCC shall ensure that a username and initial password is provided as set out in the SMKI Registration Authority Policies and Procedures (SMKI RAPP). The DCC shall ensure that the initial password must be changed by the user upon first use, and maintenance of the username and password is detailed in the SMKI Repository Code of Connection.

The DCC shall ensure that users are provided with a profile page which enables users to view and update their SMKI Repository Portal username and password and to update contact information, as set out in the SMKI Repository Code of Connection.

The DCC shall ensure that the SMKI Repository Portal interface presents to the user an x.509 v3 certificate that is recognised by the 'CA/Browser Forum' for the purposes of allowing the DCC Gateway Connection user's systems to authenticate the server as part of establishing the TLS session.

The DCC shall ensure that the SMKI Repository Portal denies access where a user does not present a valid username and password for authentication.

2.1.3 Retrieval of SMKI Repository content

The DCC shall ensure that the SMKI Repository Portal interface enables DCC Gateway Connection users to search for and download via a web form the following files that are lodged in the SMKI Repository, where they have successfully established a secured TLS connection to the SMKI Repository Portal interface (as set out in the SMKI Repository User Guide):

a) Organisation Certificates and OCA Certificates;

b) Device Certificates and DCA Certificates;

c) the latest Organisation CRL and the latest Organisation ARL; and

d) other documents lodged in the SMKI Repository.

2.2 SMKI Repository Web Service interface

2.2.1 General Obligations

The DCC shall ensure that the SMKI Repository Web Service interface enables DCC Gateway Connection users' systems to search for and obtain content lodged in the SMKI Repository, as set out in section 2.2.3, Annex A and Annex B of this document.

The DCC shall ensure that the SMKI Repository Web Service interface via DCC Gateway Connection:

a) uses the HTTPS protocol, secured by TLS in line with the protocols set out in Annex C of this document;

b) is accessed via URLs that are set out in the SMKI Repository User Guide;

c) uses Extensible Markup Language (XML) over POST for message requests and responses;

d) provides XML message responses which conform with the details set out in Annex A of this document and the XML schema set out in Annex B of this document;

e) conforms with the XML schema set out in Annex B for message requests and responses; and

f) is only accessible using a DCC Gateway Connection.

Prior to gaining access to the SMKI Repository Web Service interface, a DCC Gateway Connection user shall access the profile page on the SMKI Repository Portal in order to obtain its credentials for the SMKI Repository Web Service interface, as set out in the SMKI RAPP. The DCC shall ensure that the credentials for the SMKI Repository Web Service interface shall be in the form of an API Key, which is generated by the DCC and is a 15 character UTF-8 case insensitive string.

The DCC shall, in accordance with the SMKI RAPP, provide the DCC Gateway Connection user with a 'CA/Browser Forum' recognised certificate authority root certificate and all corresponding issuing authority certificates, for the purposes of enabling server authentication of the SMKI Repository Web Service interface.

The DCC shall ensure that each API Key shall:

a) remain valid until manually replaced by the DCC Gateway Connection user using the SMKI Repository Portal interface; and

b) once replaced, be invalid for authentication to the SMKI Repository Web Service interface.

2.2.2 Establishing connection to the SMKI Repository Web Service interface via DCC Gateway Connection

In order to establish a connection to the SMKI Repository Web Service interface, a DCC Gateway Connection user shall submit a request to establish a secured TLS session which:

a) accesses a URL as set out in section 2.2.1 of this document; and

b) includes its API Key in the querystring, in order that the SMKI Repository Interface can authenticate the user before attempting to parse the XML request document in accordance with Annex A and Annex B of this document; and

c) configures its systems such that the TLS session renegotiation timeout is set to 5 minutes.

The DCC shall ensure that the SMKI Repository Web Service presents an x.509 v3 certificate that is recognised by the 'CA/Browser Forum' referenced in section 2.2.1 of this document, for the purposes of allowing the DCC Gateway Connection user's client to authenticate the server as part of establishing the TLS session. The DCC Gateway Connection user shall verify the 'CA/Browser Forum' certificate and, if successfully verified, accept the certificate.

The DCC shall ensure that access to the SMKI Repository Web Service interface is denied where the user does not present a valid API Key for authentication.

2.2.3 Retrieval of SMKI Repository content

The DCC shall ensure that the SMKI Repository Portal Web Service interface enables DCC Gateway Connection users to search for and download the following files that are lodged in the SMKI Repository, where they have successfully established a connection to the SMKI Repository Portal Web Service interface:

a) Organisation Certificates and OCA Certificates;

b) Device Certificates and DCA Certificates;

c) the latest Organisation CRL and the latest Organisation ARL.

2.3 SSH File Transfer Protocol (SFTP) Interface

2.3.1 General Obligations

The DCC shall ensure that the SFTP Interface to the SMKI Repository enables DCC Gateway Connection users' systems to download Organisation Certificates, OCA Certificates, Device Certificates, DCA Certificates, Organisation CRLs and Organisation ARLs lodged in the SMKI Repository, as set out this section and Annex C of this document. The recommended practices for management stated in NISTIR 7966 section 5 should be followed where RFC references are shown in this section.

The DCC shall ensure that the SFTP Interface to the SMKI Repository via a DCC Gateway Connection:

a) is accessed via URLs that are set out in the SMKI Repository User Guide;

b) is implemented in a standard format:

  i. conforming to Secure Shell (SSH-2) protocol, in accordance with RFC 4251, RFC 4252 and RFC 4253;

  ii. conforming to RFC 4251, RFC 4252, RFC 4253 and RFC 959 (File Transfer Protocol) for the purposes of error handling;

iii. where the Transport Layer implements encrypted communications using the AES (Advanced Encryption Standard) cipher (FIPS-197) with a 128-bit key length, in CBC mode (aes128-cbc);

iv. where the Transport Layer implements MAC communications using hmac in accordance with RFC2104, combined with sha1 (hmac-sha1); and

v. where the Transport Layer implements RAW DSS Keys in ssh-dss format;

c) is implemented such that 'Quality of Service' constraints (rate-limiting) are applied to the download of files via the SFTP Interface to protect other aspects of the overall DCC service;

d) provides access to the files specified in section 2.3.3 of this document; and

e) is only accessible using a DCC Gateway Connection.

Prior to gaining access to the SFTP Interface to the SMKI Repository, the DCC shall provide a username and initial password to the DCC Gateway Connection user as part of the process as set out in the SMKI RAPP. The DCC shall ensure that the initial password to authenticate to the SFTP Interface shall be provided to the DCC Gateway Connection user via the profile page on the SMKI Repository Portal.

The DCC shall ensure that the initial password must be changed by the DCC Gateway Connection user upon first use, using the profile page on the SMKI Repository Portal. The DCC shall ensure that a password used to authenticate to the SFTP Interface may be changed by the DCC Gateway Connection user at any time, via the profile page on the SMKI Repository Portal. The DCC shall ensure that each password used to authenticate to the SFTP Interface shall remain valid until replaced by the DCC Gateway Connection user via the SMKI Repository Portal interface and shall be invalid thereafter.

The DCC shall provide the DCC Gateway Connection user with the DCC SSH public key, which shall be available for download/viewing in the 'Help and Support' section of the SMKI Repository Portal.

2.3.2 Establishing connection to the SFTP Interface to the SMKI Repository

In order to establish a connection to the SFTP Interface, each DCC Gateway Connection user shall:

a) make use of a standard SFTP client that supports the configuration as detailed in section 2.3.1 of this document;

b) authenticate to the SFTP interface by using a valid combination of its username and password, in accordance with the 'password' method; and

c) verify that the DCC SSH public key, as provided by the DCC as set out in section 2.3.1 of this document, matches the details within the SMKI Repository Portal prior to using the SFTP Interface.

Details of how a DCC Gateway Connection user should configure its SFTP client are set out in the SMKI Repository User Guide.

2.3.3 Retrieval of SMKI Repository content

The DCC shall ensure that the SFTP interface enables DCC Gateway Connection users' systems to download the following files that are lodged in the SMKI Repository, where they have successfully established a connection to the SFTP Interface:

a) a file in .gz format and having a name of form *SMKIKR_FULL_YYYY-MM-DD.xml.gz*, updated weekly by the time set out in the SMKI Repository User Guide, containing:

   i. an XML file which complies with the SMKI Repository Web Service interface schema as set out in Annex B of this document, having a name of the form SMKIKR_FULL_YYYY-MM-DD.xml and which contains certificates, comprising OCA Certificates, DCA Certificates, Organisation Certificates and Device Certificates with a status of 'In-Use'.

b) seven files in .gz format and having names of the form *SMKIKR_DELT_YYYY-MM-DD.xml.gz*, updated daily, each of which contains:

   i. an XML file which complies with the SMKI Repository Web Service interface schema as set out in Annex B of this document, having a name of the form SMKIKR_DELT_YYYY-MM-DD.xml and which contains certificates comprising OCA Certificates, DCA Certificates, Organisation Certificates, and Device Certificates Issued and lodged in the SMKI Repository during the preceding twenty four hours or whose Certificate status has change. This will enable the user to maintain a daily synchronised copy of the certificates in the SMKI Repository. Each of the seven daily files shall be available for 7 days from publication and shall then be removed by the DCC from the SMKI Repository.

c) a file with extension 'gz' that is the latest Organisation ARL;

d) a file with extension 'gz' that is the latest Organisation CRL;

e) a file in .gz format, updated as necessary, containing the base set of Organisation Certificates and OCA Certificates required to populate Device anchor slots prior to installation for the North Region; and

f) a file in .gz format, updated as necessary, containing the base set of Organisation Certificates and OCA Certificates required to populate Device anchor slots prior to installation for the Central Region and South Region.

The DCC shall ensure that the files holding certificates are made available in .gz format, with all versions of .gz being supported. Each .gz file will contain a single XML file which complies with the XML schema as set out in Annex B, containing individual certificates, represented as Base64 encoded strings.

The DCC shall ensure that the Organisation Certificates and OCA Certificates contained within the two files at (e) and (f) above shall be the same, other than the Organisation Certificates for the Remote Party Role of wanProvider, with its GBCS meaning.

The DCC shall lodge a document in the SMKI Repository, which sets out details of which of the base set of Organisation Certificates and OCA Certificates may be placed in specific Device Trust Anchor Cells, where that term has its GBCS meaning.

Annex A: SMKI Repository Web Service interface specification

Response Codes

The DCC shall ensure that the following HTTP response codes are returned in the response to each attempted access to the SMKI Repository Web Service interface:

a) HTTP response code 200, where a request is successful;

b) HTTP response code 4xx (400-499) where there is an error that is anticipated;

c) HTTP response code 404, where a request is made but the User should not have access to the SMKI Repository Web Service interface; and

d) HTTP response code 5xx (500-599) for unanticipated error conditions.

Response codes are also replicated in the XML response body as **ResponseCode**, along with a human readable description as **ResponseMessage** as set out in the 'Service Specific Error Codes' sections within this Annex A.

Audit References

Each response shall include an **AuditReference** entity in each response body. This is a globally unique reference for the request served, and can be considered both as a receipt reference and a diagnostic tool in relation to the investigation of problems encountered in using the SMKI Repository Web Service.

HTTP POST Certificate Search

The table immediately below sets out the way in which a user may search the SMKI Repository by means of the SMKI Repository Web Service interface.

Web Service URL	**/services/certificatesearch**
Required Parameters	apikey=*<SRI User's API Key>*
Example URL	https://site.name.com/services/certificatesearch?apikey=u3bg9gt38htd0j2
Required POST	UTF8 encoded XML v1.0 document with a top level **CertificateSearchRequest** entity, containing search term entities from the following list: • **CertificateSubjectName** (23 character EUI-64 format in the case of it being the Unique Identifier for an organisation or other up to 23 character subject name in the case of it being the common name of an OCA or DCA Certificate) • **CertificateSubjectAltName** (23 character EUI-64 format) • **CertificateSerial** (Up to 50 character string) • **CertificateStatus** (1 character string) • **PubDateRangeStart** (yyyy-mm-dd) • **PubDateRangeEnd** (yyyy-mm-dd)

	• **ExpDateRangeStart** (yyyy-mm-dd) • **ExpDateRangeEnd** (yyyy-mm-dd) • **RevDateRangeStart** (yyyy-mm-dd) • **RevDateRangeEnd** (yyyy-mm-dd) • **InUseDateRangeStart** (yyyy-mm-dd) • **InUseDateRangeEnd** (yyyy-mm-dd) • **CertificateIssuer** (Up to 23 character string) • **CertificateRole** (Integer) • **ManufacturingFlag** (true/false) All search term entities are optional, but it is mandatory to provide either **CertificateSubjectName**, **CertificateSubjectAltName** or **CertificateSerial**

Example Request XML	`<?xml version="1.0" encoding="utf-8"?>`
	`<CertificateSearchRequest>`
	`<CertificateSubjectAltName>01-02-03-04-05-06-07-08</CertificateSubjectAltName>`
	`<PubDateRangeStart>2014-01-01</PubDateRangeStart>`
	`<PubDateRangeEnd>2018-01-01</PubDateRangeEnd>`
	`</CertificateSearchRequest>`

Response Format	UTF8 encoded XML v1.0 document with a top level **CertificateSearchResponse** entity, containing the following entities: • **ResponseCode** (up to 3 character string) • **ResponseMessage** (up to 50 character string) • **AuditReference** (up to 20 character string) Followed by a variable number of **Result** entities (in the case of a successful response), each comprising: • **CertificateSerial** (Up to 50 character string) • **CertificateSubjectAltName** (23 character EUI-64 format) • **CertificateSubjectName** (23 character EUI-64 format or other up to 23 character subject name in the case of a DCA or OCA Certificate common name) • **CertificateStatus** (1 character string) • **CertificateRole** (Integer) • **CertificateUsage** (2 character string) • **ManufacturingFlag** (true/false)

Example Response XML	`<?xml version="1.0" encoding="utf-8"?>`
	`<CertificateSearchResponse>`
	`<ResponseCode>200</ResponseCode>`
	`<ResponseMessage>Success</ResponseMessage>`
	`<AuditReference>1234567890-abc123456</AuditReference>`
	`<Result>`
	`<CertificateSerial>00926EAABE07B701DF</CertificateSerial>`

	<CertificateSubjectAltName>01-02-03-04-05-06-07-08</CertificateSubjectAltName> <CertificateStatus>I</CertificateStatus> <CertificateRole>2</CertificateRole> <CertificateUsage>DS</CertificateUsage> <ManufacturingFlag>false</ManufacturingFlag> </Result> <Result> <CertificateSerial>1234567890</CertificateSerial> <CertificateSubjectAltName>01-02-03-04-05-06-07-08</CertificateSubjectAltName> <CertificateStatus>P</CertificateStatus> <CertificateRole>2</CertificateRole> <CertificateUsage>DS</CertificateUsage> <ManufacturingFlag>false</ManufacturingFlag> </Result> </CertificateSearchResponse>
Service Specific Error Codes	**401** = Invalid Search Parameters **402** = No Certificates Match Search Parameters
Notes	

Retrieve Certificate

The table immediately below sets out the way in which a user may retrieve a certificate from the SMKI Repository by means of the SMKI Repository Web Service interface.

Web Service URL	*/services/retrievecertificate*
Required Parameters	apikey=<*SRI User's API Key*>
Example URL	https://site.name.com/services/retrievecertificate?apikey=u3bg9gt38htd0j2
Required POST	UTF8 encoded XML v1.0 document with a top level **CertificateDataRequest** entity, containing the following, mandatory, entity: - **CertificateSerial** (Up to 50 character string)
Example Request XML	<?xml version="1.0" encoding="utf-8"?> <CertificateDataRequest> <CertificateSerial>00926EAABE07B701DF</CertificateSerial> </CertificateDataRequest>
Response Format	UTF8 encoded XML v1.0 document with a top level **CertificateSearchResponse** entity, containing the following entities: - **ResponseCode** (up to 3 character string)

	• **ResponseMessage** (up to 50 character string) • **AuditReference** (up to 20 character string) • **CertificateResponse** (in the case of a successful response) consisting of: ○ **CertificateSubjectName** (23 character EUI-64 format in the case of it being the Unique Identifier for an organisation or other up to 23 character subject name in the case of the common name of a DCA or OCA Certificate) ○ **CertificateSubjectAltName** (23 character string) ○ **CertificateSerial** (Up to 50 character string) ○ **CertificateStatus** (1 character string) ○ **CertificateBody** (Base64 representation of the DER encoded ASN.1 notated certificate data) ○ **CertificateRole** (Integer) ○ **CertificateUsage** (2 character string) ○ **ManufacturingFlag** (true/false)

Example Response XML	<?xml version="1.0" encoding="utf-8"?>
	<CertificateDataResponse>
	  <ResponseCode>200</ResponseCode>
	  <ResponseMessage>Success</ResponseMessage>
	  <AuditReference>1234567890-abc123456</AuditReference>
	  <CertificateResponse>
	    <CertificateSubjectAltName>01-02-03-04-05-06-07-08</CertificateAltName>
	    <CertificateSerial>00926EAABE07B701DF</CertificateSerial>
	    <CertificateStatus>I</CertificateStatus>
	    <CertificateBody>
	      (base64 certificate data)
	    </CertificateBody>
	    <CertificateRole>2</CertificateRole>
	    <CertificateUsage>DS</CertificateUsage>
	    <ManufacturingFlag>false</ManufacturingFlag>
	  </CertificateResponse>
	</CertificateDataResponse>

Service Specific Error Codes	**401** = Invalid Input Parameters **402** = No Certificates Match Input Parameters **403** = No Matching Certificates Are Valid
Notes	Certificates are requested by serial number, and serial numbers are globally unique across the SMKI. Therefore only one certificate (i.e. one CertificateResponse entity) will be returned. The certificatesearch service should be used to determine the serial number for the certificate required.

Organisation CRL and Organisation ARL Retrieval

The latest version of the Organisation CRL and Organisation ARL shall be available from separate static URLs enabling the automation of the CRL or ARL download via the SMKI Repository Web Service interface. Informational text will be displayed on the Portal to inform the user how users may automate downloads of these files using URLs of the form /revocationlists/<common_name>?apikey=<user_api_key>. The actual URL shall be detailed in the SMKI Repository User Guide.

Meaning of XML schema codes

The table immediately below sets out the meaning of codified elements with the XML schema for the SMKI Repository Web Service Interface, where such XML schema is as set out in Annex B of this document.

XML Schema Element Name	Possible Values	Meaning
CertificateStatus	P I N E R	Pending In use Not In use Expired Revoked
ManufacturingFlag	true false	Can be used during manufacturing Cannot be used during manufacturing
CertificateUsage	DS KA CS	Digital Signing Key Agreement Certificate Signing
CertificateRole	See 'Remote Party Role Code' in Annex A of Section L	See corresponding 'Remote Party Role' in Annex A of Section L

Annex B: SMKI Repository Web Service interface schema

This section specifies the XML schema that must be used for the SMKI Repository Web Service, as set out immediately below.

The DCC shall ensure that the version number of the SMKI Repository Web Service interface is contained within the XML schema, as set out below. Each user of the SMKI Repository Web Service interface shall ensure that the version number is included within:

a) the URL used to access the SMKI Repository Web Service interface;

b) the schema filename; and

c) XML requests and responses.

There shall be a different end point for each version of the SMKI Repository Web Service interface. Different versions shall be supported on separate URLs.

```
<?xml version="1.0" encoding="UTF-8"?>
<xs:schema xmlns:xs="http://www.w3.org/2001/XMLSchema" elementFormDefault="qualified">
  <!--
Version (string)
  -->
        <xsd:element name="Version">
            <xsd:simpleType>
             <xsd:restriction base="xsd:string">
               <xsd:enumeration value="1.0"/>
             </xsd:restriction>
           </xsd:simpleType>
  <!--
  ResponseCode (up to 3 character string)
  -->
  <xs:simpleType name="ResponseCode">
        <xs:restriction base="xs:string">
                <xs:maxLength value="3"/>
                <xs:minLength value="1"/>
        </xs:restriction>
  </xs:simpleType>
  <!--
  ResponseMessage (up to 50 character string)
  -->
  <xs:simpleType name="ResponseMessage">
        <xs:restriction base="xs:string">
                <xs:maxLength value="50"/>
                <xs:minLength value="1"/>
        </xs:restriction>
  </xs:simpleType>
  <!--
  AuditReference (up to 20 character string)
  -->
  <xs:simpleType name="AuditReference">
        <xs:restriction base="xs:string">
                <xs:maxLength value="20"/>
                <xs:minLength value="1"/>
        </xs:restriction>
  </xs:simpleType>
<!--
  Status (1 character enum values: S = Success, F = Failure)
 -->
  <xs:simpleType name="Status">
        <xs:restriction base="xs:string">
                <xs:enumeration value="S"/>
                <xs:enumeration value="F"/>
        </xs:restriction>
  </xs:simpleType>
  <xs:element name="ResponseCode" type="ResponseCode"/>
  <xs:element name="ResponseMessage" type="ResponseMessage"/>
  <xs:element name="AuditReference" type="AuditReference"/>
!--
        CertificateSubjectName (23 character EUI-64 format)
-->
```

```
  <xs:simpleType name="CertificateSubjectName">
              <xs:restriction base="xs:string">
                          <xs:maxLength value="23"/>
                          <xs:minLength value="1"/>
              </xs:restriction>
  </xs:simpleType>
<!--
              CertificateSubjectAltName (23 character string)
-->
  <xs:simpleType name="CertificateSubjectAltName">
              <xs:restriction base="xs:string">
                          <xs:maxLength value="23"/>
                          <xs:minLength value="1"/>
              </xs:restriction>
  </xs:simpleType>
<!--
              CertificateStatus (1 character string)
-->
  <xs:simpleType name="CertificateStatus">
              <xs:restriction base="xs:string">
                          <xs:enumeration value="P"/>
                          <xs:enumeration value="I"/>
                          <xs:enumeration value="N"/>
                          <xs:enumeration value="E"/>
                          <xs:enumeration value="R"/>
              </xs:restriction>
  </xs:simpleType>
<!--
              PubDateRangeStart (yyyy-mm-dd)
-->
  <xs:simpleType name="PubDateRangeStart">
     <xs:restriction base="xs:date"/>
  </xs:simpleType>
<!--
              PubDateRangeEnd (yyyy-mm-dd)
-->
  <xs:simpleType name="PubDateRangeEnd">
     <xs:restriction base="xs:date"/>
  </xs:simpleType>
<!--
              ExpDateRangeStart (yyyy-mm-dd)
-->
  <xs:simpleType name="ExpDateRangeStart">
     <xs:restriction base="xs:date"/>
  </xs:simpleType>
<!--
              ExpDateRangeEnd (yyyy-mm-dd)
-->
  <xs:simpleType name="ExpDateRangeEnd">
     <xs:restriction base="xs:date"/>
  </xs:simpleType>
<!--
              RevDateRangeStart (yyyy-mm-dd)
-->
  <xs:simpleType name="RevDateRangeStart">
     <xs:restriction base="xs:date"/>
  </xs:simpleType>
<!--
              RevDateRangeEnd (yyyy-mm-dd)
-->
  <xs:simpleType name="RevDateRangeEnd">
     <xs:restriction base="xs:date"/>
  </xs:simpleType>
<!--
              InUseDateRangeStart(yyyy-mm-dd)
-->
  <xs:simpleType name="InUseDateRangeStart">
     <xs:restriction base="xs:date"/>
  </xs:simpleType>
<!--
              InUseDateRangeEnd(yyyy-mm-dd)
-->
  <xs:simpleType name="InUseDateRangeEnd">
     <xs:restriction base="xs:date"/>
  </xs:simpleType>
```

```
<!--
        CertificateIssuer (23 character string)
-->
 <xs:simpleType name="CertificateIssuer">
        <xs:restriction base="xs:string">
                <xs:maxLength value="23"/>
                <xs:minLength value="1"/>
        </xs:restriction>
 </xs:simpleType>
<!--
 CertificateSerial (50 character string)
-->
 <xs:simpleType name="CertificateSerial">
        <xs:restriction base="xs:string">
                <xs:maxLength value="50"/>
                <xs:minLength value="1"/>
        </xs:restriction>
 </xs:simpleType>
<!--
 Result
-->
  <xs:complexType name="Result">
   <xs:sequence>
    <xs:element name="CertificateSerial" type="CertificateSerial" minOccurs="1" maxOccurs="1"/>
    <xs:element name="CertificateSubjectAltName" type="CertificateSubjectAltName" minOccurs="0"
maxOccurs="1"/>
    <xs:element name="CertificateSubjectName" type="CertificateSubjectName" minOccurs="0" maxOccurs="1"/>
    <xs:element name="CertificateStatus" type="CertificateStatus" minOccurs="1" maxOccurs="1"/>
        <xs:element name="CertificateRole" type="xs:integer" minOccurs="0" maxOccurs="1"/>
        <xs:element name="CertificateUsage" type="CertificateUsage" minOccurs="1" maxOccurs="1"/>
        <xs:element name="ManufacturingFlag" type="xs:boolean" minOccurs="1" maxOccurs="1"/>
   </xs:sequence>
  </xs:complexType>
<!--
        CertificateResponse (in the case of a successful response) consisting of:
-->
  <xs:complexType name="CertificateResponse">
   <xs:sequence>
    <xs:element name="CertificateSubjectName" type="CertificateSubjectName" minOccurs="0" maxOccurs="1"/>
    <xs:element name="CertificateSubjectAltName" type="CertificateSubjectAltName" minOccurs="0"
maxOccurs="1"/>
    <xs:element name="CertificateSerial" type="CertificateSerial" minOccurs="1" maxOccurs="1"/>
    <xs:element name="CertificateStatus" type="CertificateStatus" minOccurs="1" maxOccurs="1"/>
    <xs:element name="CertificateBody" type="xs:base64Binary" minOccurs="0" maxOccurs="1"/>
                <xs:element name="CertificateRole" type="xs:integer" minOccurs="0" maxOccurs="1"/>
        <xs:element name="CertificateUsage" type="CertificateUsage" minOccurs="1" maxOccurs="1"/>
        <xs:element name="ManufacturingFlag" type="xs:boolean" minOccurs="1" maxOccurs="1"/>
   </xs:sequence>
  </xs:complexType>

<!--
        CertificateDataRequest
-->
 <xs:complexType name="CertificateDataRequest">
  <xs:sequence>
           <xs:element name="CertificateSerial" type="CertificateSerial" minOccurs="1" maxOccurs="1"/>
  </xs:sequence>
 </xs:complexType>
<!--
        CertificateUsage (2 character string)
-->
 <xs:simpleType name="CertificateUsage">
        <xs:restriction base="xs:string">
                <xs:enumeration value="DS"/>
                <xs:enumeration value="KA"/>
                <xs:enumeration value="CS"/>
        </xs:restriction>
 </xs:simpleType>
<!--
        CertificateDataResponse
-->
 <xs:complexType name="CertificateDataResponse">
  <xs:sequence>
   <xs:element name="ResponseCode" type="ResponseCode" minOccurs="1" maxOccurs="1"/>
   <xs:element name="ResponseMessage" type="ResponseMessage" minOccurs="1" maxOccurs="1" />
   <xs:element name="AuditReference" type="AuditReference" minOccurs="1" maxOccurs="1"/>
   <xs:element name="CertificateResponse" type="CertificateResponse" minOccurs="0"
maxOccurs="unbounded"/>
  </xs:sequence>
 </xs:complexType>
<!--
        CertificateSearchRequest. Note: At least one of CertificateSerial, CertificateSubjectName or
CertificateSubjectAltName must be supplied. This is not enforced by the XSD, but is enforced by the SMKI
Repository code.
-->
 <xs:complexType name="CertificateSearchRequest">
  <xs:sequence>
    <xs:element name="CertificateSerial" type="CertificateSerial" minOccurs="0" maxOccurs="1"/>
    <xs:element name="CertificateSubjectName" type="CertificateSubjectName" minOccurs="0" maxOccurs="1"/>
    <xs:element name="CertificateSubjectAltName" type="CertificateSubjectAltName" minOccurs="0"
maxOccurs="1"/>
    <xs:element name="CertificateStatus" type="CertificateStatus" minOccurs="0" maxOccurs="1"/>
    <xs:element name="PubDateRangeStart" type="PubDateRangeStart" minOccurs="0" maxOccurs="1"/>
    <xs:element name="PubDateRangeEnd" type="PubDateRangeEnd" minOccurs="0" maxOccurs="1"/>
    <xs:element name="ExpDateRangeStart" type="ExpDateRangeStart" minOccurs="0" maxOccurs="1"/>
    <xs:element name="ExpDateRangeEnd" type="ExpDateRangeEnd" minOccurs="0" maxOccurs="1"/>
    <xs:element name="RevDateRangeStart" type="RevDateRangeStart" minOccurs="0" maxOccurs="1"/>
    <xs:element name="RevDateRangeEnd" type="RevDateRangeEnd" minOccurs="0" maxOccurs="1"/>
    <xs:element name="InUseDateRangeStart" type="InUseDateRangeStart" minOccurs="0" maxOccurs="1"/>
    <xs:element name="InUseDateRangeEnd" type="InUseDateRangeEnd" minOccurs="0" maxOccurs="1"/>
        <xs:element name="CertificateIssuer" type="CertificateIssuer" minOccurs="0" maxOccurs="1"/>
        <xs:element name="CertificateRole" type="xs:integer" minOccurs="0" maxOccurs="1"/>
        <xs:element name="ManufacturingFlag" type="xs:boolean" minOccurs="0" maxOccurs="1"/>
  </xs:sequence>
 </xs:complexType>
<!--
        CertificateSearchResponse
-->
 <xs:complexType name="CertificateSearchResponse">
  <xs:sequence>
   <xs:element name="ResponseCode" type="ResponseCode" minOccurs="1" maxOccurs="1"/>
   <xs:element name="ResponseMessage" type="ResponseMessage" minOccurs="1" maxOccurs="1"/>
   <xs:element name="AuditReference" type="AuditReference" minOccurs="1" maxOccurs="1"/>
   <xs:element name="Result" type="Result" minOccurs="0" maxOccurs="unbounded"/>
  </xs:sequence>
 </xs:complexType>
 <xs:element name="CertificateDataRequest" type="CertificateDataRequest"/>
 <xs:element name="CertificateDataResponse" type="CertificateDataResponse"/>
 <xs:element name="CertificateSearchRequest" type="CertificateSearchRequest"/>
 <xs:element name="CertificateSearchResponse" type="CertificateSearchResponse"/>
</xs:schema>
```

Annex C: Authentication Credentials

The SMKI Repository Portal Interface via DCC Gateway Connection, SMKI Repository Web Service interface and SFTP interface shall use server certificates with the following properties:

Criteria	***Version***
Protocol	*TLS**
Protocol Cyphers	*ECDHE-RSA-AES256-GCM-SHA384*
	ECDHE-RSA-AES128-GCM-SHA256
	ECDHE-RSA-AES128-SHA256
Client Certificate Key	*RSA 2048 bit*
Client Certificate Hash Algorithm	*SHA256*
Server Certificate Key	*RSA 2048 bit*
Server Certificate Hash Algorithm	*SHA256*

* TLS should be implemented in accordance with Java and Apache standards and the SMKI PMA and SSC Guidance (Standards, Procedures and Guidelines) published on the SEC website. The TLS version is specified in the HTTP client protocol initialisation. To enable AES256, the Java runtime should be patched with “JCE Unlimited Strength Jurisdiction Policy Files” for the version of Java being used. This is obtained from the public Oracle Java download web pages.

Annex D: Definitions

Term	Meaning as defined in SEC
In-Use	Means a valid Device Certificate that has not been operationally superseded and which the Device has acknowledged as being successful installed/updated
SMKI Repository Portal	Means an interface accessed via a web browser, as set out in section 2.1 of this document.
SMKI Repository User Guide	Means the document published pursuant to section 2.1 of this document.
SMKI Repository Web Service	Means an interface that can be accessed by a Party's or an RDP's systems, as set out in section 2.2, Annex A and Annex B of this document.
SSH File Transfer Protocol Interface (the "SFTP Interface")	Means an interface that can be accessed via an SFTP client, as set out in section 2.3 of this document.
Uniform Resource Locator (URL)	Has the meaning at https://en.wikipedia.org/wiki/URL

Version: P2.0

APPENDIX P

SMKI Repository Code of Connection

Purpose and Scope

This SMKI Repository Code of Connection is the document required by Section L6.5 of the SEC.

1. Connection Mechanism

1.1. Interface access

DCC Gateway Connection users may connect to the SMKI Repository interfaces as set out in sections 3.1 to 3.3 of this document, via that DCC Gateway Connection, and where they have been issued with credentials to authenticate to such SMKI Repository interfaces. The means by which a connection is made to the SMKI Repository interfaces is set out in the SMKI Repository Interface Design Specification.

Any Party or RDP without a DCC Gateway Connection may access SMKI Repository content as set out in section 2.2 of this document and the SMKI Repository Interface Design Specification.

1.2. Browser Policy

The DCC shall publish and keep up to date the web browsers and versions which the SMKI Repository Portal Interface supports.

Browsers and versions other than those published may also be compatible, though they will not be supported and access to the SMKI Repository Portal interface using other such browsers and versions cannot be guaranteed. No browsers shall be explicitly blocked or denied access to the SMKI Repository Portal interface, though there may be unexpected behaviour when a browser or version other than those published is used.

The browsers supported by the DCC shall be reviewed from time to time. Except as set out in the paragraph below, the DCC shall seek views from Parties or RDPs with access to the SMKI Repository Portal interface prior to the withdrawal of support for any browser or version previously published.

The DCC shall not be required to support browser versions that are not supported by that browser's vendor.

1.3. Lodging Information in the SMKI Repository

The DCC shall ensure that any persons as set out in Section L5.3 of the SEC may lodge information in the SMKI Repository. Such persons acting on behalf of the SMKI PMA or the Code Administrator must be an ARO and shall contact the Service Desk in order to lodge information into the SMKI Repository.

Prior to lodging any such information in the SMKI Repository on behalf of the SMKI PMA or the Code Administrator, the DCC shall authenticate the identity of the ARO wishing to lodge information in the SMKI Repository by confirming such information from the relevant ARO Nomination Form, in order to provide confidence that the request is from an authorised ARO.

The DCC shall lodge all information in the SMKI Repository as soon as is practicable upon receipt, subject to the above identity checks.

2. SMKI Repository interfaces

2.1. Not used

2.2. SMKI Repository content access for users without a DCC Gateway Connection

Parties, RDPs or representatives of the SMKI PMA, Panel or Code Administrator wishing to obtain information lodged in the SMKI Repository, other than via a DCC Gateway Connection, may do so by contacting the Service Desk as set out in the SMKI Repository User Guide, via personal visit, e-mail, signed fax, signed letter or telephone for the purposes of viewing, and/or obtaining a copy of a document lodged in the SMKI Repository. Following such contact, the DCC shall ensure that the relevant requested copies of Certificates or other information is provided via optical media such as CD, DVD or, where appropriate, email.

Parties or RDPs may also access the SMKI Portal via the Internet to retrieve SMKI Repository content, as set out in the SMKI Interface Design Specification.

3. Authentication

The DCC shall ensure that credentials to access the SMKI Repository interfaces are provided, following successful completion of the registration processes required to become an ARO, as set out in the SMKI RAPP.

Access to the SMKI Repository interfaces for persons who do not have access to a DCC Gateway Connection is set out in section 2.2 of this document.

3.1. Authentication to the SMKI Repository Portal interface

The DCC shall provide DCC Gateway Connection users with a username and password in accordance with the SMKI RAPP. Upon first login or after a password reset completed by the DCC, the DCC Gateway Connection user shall be required to ensure that the ARO's account password is changed via the SMKI Repository Portal, as set out in the SMKI Repository User Guide.

If the DCC Gateway Connection users enters an incorrect password five times within a one hour period, the DCC shall ensure that the account will automatically lock for one hour from the first failed authentication attempt, or until it is manually unlocked by an administrator on request by an ARO to the DCC Service Desk. Upon request from an ARO to unlock its SMKI Repository Portal interface password, the DCC shall authenticate the identity of the ARO by confirming such information from the relevant ARO Nomination Form, in order to provide confidence that the request is from an authorised ARO.

3.2. Not used

3.3. Not used

4. Managing Demand

Each DCC Gateway Connection user shall provide a forecast of the number of certificates that the DCC Gateway Connection user anticipates retrieving from any SMKI Repository Interface either individually or in bulk. Such forecasts shall be a reasonable estimate of the DCC Gateway Connection user's intended usage. The scope of requests in relation to which a forecast is required is set out in Appendix A of this document.

Each DCC Gateway Connection user shall take all reasonable steps to ensure that their usage does not exceed 120% of their forecast in Table 1.

When a DCC Gateway Connection user's actual number of requests for a particular type of access, as set out in Table 1, to the SMKI Repository exceeds 120% of its forecast, the DCC Service Desk may inform the DCC Gateway Connection user via secured electronic means as set out in the SMKI Repository User Guide.

Each DCC Gateway Connection user shall notify the DCC Service Desk of any short term or long term usage which is expected to exceed 120% of its forecast and the DCC shall make reasonable attempts to meet this additional demand which may include proposal of a schedule when this additional demand can be met without adversely affecting the provision of the service.

4.1. Error Responses

In cases where there is a failure of the service or infrastructure, or a delay in the processing of a request that causes the DCC Gateway Connection user's browser or a device upstream of the SMKI Repository Interface to abandon the request before the SMKI Repository Interface begins to execute the request, the generation or delivery of a SMKI Repository Interface error message may not be possible.

Appendix A Templates for Information to be supplied by Parties

Each DCC Gateway Connection user shall provide to the DCC via the DCC Service Desk, using the mechanism as set out in the SMKI Repository User Guide, the forecast information identified in this Appendix in regard to their proposed use of the DCC Gateway Connection user's connection to the SMKI Repository.

1. Usage Forecast

DCC Gateway Connection users shall forecast their usage of the SMKI Repository in relation to the request types in the table below.

The first table identifies the forecasts required of the number of requests for web services requests and SMKI Repository Portal requests.

Request type	Maximum Number of Requests per 24 hour period
SMKI Repository Web Service interface requests	< value >
SMKI Repository Portal interface requests	< value >

Table 1 Daily Usage Forecast

An assumption has been made that the daily delta file will be downloaded by each DCC Gateway Connection user each day and one download of the full database file per week. DCC Gateway Connection users shall enter the day of the week that they will download the full database file. All additional attempts to download the delta file or full database file or attempts to download the database file outside of the agreed day must be communicated and agreed with the DCC. The DCC shall make reasonable attempts to meet this additional demand, or change in schedule, which may include proposing a day and time frame when this will be possible without adversely affecting the provision of the service.

Request type	Download Day
SFTP Full Download	< Day >

Table 2 SFTP Full Download Forecast

The following table is provided for the DCC Gateway Connection users to set out their forecast of the reasonable maximum usage during any 24 hour period.

	Off Peak		Core	Non-Core (evening)
Mode of Operation	00:00 – 07:00	07:00 - 08:00	08:00 - 20:00	20:00 – 00:00
SMKI Repository Portal interface requests	< Percentage of total requests via SMKI Repository Portal interface>	< Percentage of total requests via SMKI Repository Portal interface>	< Percentage of total requests via SMKI Repository Portal interface>	< Percentage of total requests via SMKI Repository Portal interface>
SMKI Repository Web Service interface requests	< Percentage of total requests via SMKI Repository Web Service interface >	< Percentage of total requests via SMKI Repository Web Service interface >	< Percentage of total requests via SMKI Repository Web Service interface >	< Percentage of total requests via SMKI Repository Web Service interface >
SFTP interface daily delta file request	< Percentage of total requests to download delta files>	< Percentage of total requests to download delta files >	< Percentage of total requests to download delta files >	< Percentage of total requests to download delta files >
SFTP interface full file request	< Percentage of total requests to download full files>	< Percentage of total requests to download full files>	< Percentage of total requests to download full files>	< Percentage of total requests to download full files>

Table 3 % of Daily Forecast

Appendix B Definitions

Term	Meaning as defined in SEC
API Key	Means an application programming interface key, used for the purposes of identifying the user of the SMKI Repository Web Service interface

Version Q7.0

APPENDIX Q

IKI Certificate Policy

(IKI CP)

CONTENTS

1 INTRODUCTION

The document comprising this Appendix Q (together with its Annexes A and B):

- shall be known as the "IKI Certificate Policy" (and in this document is referred to simply as the "Policy"); and
- is a SEC Subsidiary Document related to Section L9 of the Code (The SMKI Document Set).

1.1 OVERVIEW

(A) This Policy sets out the arrangements relating to:

(i) IKI Certificates; and

(ii) IKI Certificate Authority (ICA) Certificates.

(B) This Policy is structured according to the guidelines provided by IETF RFC 3647, with appropriate extensions, modifications and deletions.

(C) Except where the context otherwise requires, words or expressions used in this Policy shall have the meanings ascribed to them in IETF RFC 5280 where they:

(i) appear in `Courier New` font;

(ii) are accompanied by the descriptor 'field', 'type' or 'extension'; and/or

(iii) take the form of a conjoined string of two or more words, such as 'digitalSignature'.

1.2 DOCUMENT NAME AND IDENTIFICATION

(A) This Policy has been assigned an OID of 1.2.826.0.1.8641679.1.2.1.3

1.3 SMKI PARTICIPANTS

1.3.1 The IKI Root Certification Authority

(A) The definition of IKI Certification Authority is set out in Annex A.

1.3.2 Registration Authorities

(A) The definition of Registration Authority is set out in Annex A.

1.3.3 Subscribers

(A) In accordance with Section L3.20 of the Code (IKI Certificates), certain Parties, Manufacturers, RDPs and SECCo may become Authorised Subscribers.

(B) In accordance with Section L3 of the Code (The SMKI Services), an Authorised Subscriber shall be an Eligible Subscriber in relation to certain Certificates.

(C) The SMKI RAPP sets out the procedure to be followed by an Eligible Subscriber in order to become a Subscriber for one or more Certificates.

(D) Eligible Subscribers are subject to the applicable requirements of the SMKI RAPP and Section L11 of the Code (Subscriber Obligations).

(E) Obligations on the DCC acting in the capacity of an Eligible Subscriber are set out in Section L11 of the Code (Subscriber Obligations).

(F) The definitions of the following terms are set out in Section A of the Code (Definitions and Interpretation):

(i) Authorised Subscriber; and

(ii) Subscriber.

(G) Eligible Subscribers are defined in Annex A of this Policy.

1.3.4 Subjects

(A) The Subject of an IKI Certificate shall be an entity or object which may be an individual, organisation or System and must be identified in the `subject` field of the IKI Certificate Profile in accordance with Annex B.

(B) The Subject of an ICA Certificate must be the entity named in the `subject` field of the Root ICA Certificate Profile or Issuing ICA Certificate Profile (as the case may be) in accordance with Annex B.

(C) The definition of Subject is set out in Annex A.

1.3.5 Relying Parties

(A) In accordance with Section L12 of the Code, certain Parties may be Relying Parties.

(B) Relying Parties are subject to the applicable requirements of Section L12 of the Code (Relying Party Obligations).

(C) Obligations on the DCC acting in the capacity of a Relying Party are set out in Section L12 of the Code (Relying Party Obligations).

(D) The definition of Relying Party is set out in Annex A.

1.3.6 (E) The only Relying Party for IKI Certificates and ICA Certificates is the DCC.SMKI Policy Management Authority

(A) Provision in relation to the SMKI PMA is made in Section L1 of the Code (SMKI Policy Management Authority).

1.3.7 SMKI Repository Provider

(A) Provision in relation to the SMKI Repository Service is made in Section L5 of the Code (The SMKI Repository Service).

1.4 USAGE OF IKI CERTIFICATES AND ICA CERTIFICATES

1.4.1 Appropriate Certificate Uses

(A) The ICA shall ensure that IKI Certificates are Issued only:

(i) to Eligible Subscribers; and

(ii) for the purposes of either authenticating the Subject to the SMKI Services or signing files related to Threshold Anomaly Detection, the Certified Products List and the SMKI Recovery Procedure that are sent to the DCC.

(B) The ICA shall ensure that ICA Certificates are Issued only to the ICA:

(i) in its capacity as, and for the purposes of, exercising the functions of, the Root ICA; and

(ii) in its capacity as, and for the purposes of, exercising the functions of, an Issuing ICA.

(C) Further provision in relation to the use of Certificates is made in Section L11 (Subscriber Obligations) and Section L12 (Relying Party Obligations) of the Code.

1.4.2 Prohibited Certificate Uses

(i) No Party, Manufacturer, RDP or SECCo shall use a Certificate other than for the purposes specified in Part 1.4.1 of this Policy.

1.5 POLICY ADMINISTRATION

1.5.1 Organisation Administering the Document

(i) This Policy is a SEC Subsidiary Document and is administered as such in accordance with the provisions of the Code.

1.5.2 Contact Person

(i) Questions in relation to the content of this Policy should be addressed to the ICA or the SMKI PMA.

1.5.3 Person Determining IKI CPS Suitability for the Policy

(i) Provision is made in Section L9.21 of the Code for the SMKI PMA to approve the IKI CPS.

1.5.4 IKI CPS Approval Procedures

(i) Provision is made in Section L9.21 of the Code for the procedure by which the SMKI PMA may approve the IKI CPS.

1.5.5 Registration Authority Policies and Procedures

(i) The SMKI Registration Authority Policies and Procedures (the SMKI RAPP) are set out at Appendix D of the Code.

1.6 DEFINITIONS AND ACRONYMS

1.6.1 Definitions

(i) Definitions of the expressions used in this Policy are set out in Section A of the Code (Definitions and Interpretation) and Annex A.

1.6.2 Acronyms

(i) Any acronyms used for the purposes of this Policy are set out in Section A of the Code (Definitions and Interpretation) and Annex A.

2 PUBLICATION AND REPOSITORY RESPONSIBILITIES

2.1 REPOSITORIES

Provision is made in Section L5 of the Code (The SMKI Repository Service) for the establishment, operation and maintenance of the SMKI Repository.

2.2 PUBLICATION OF CERTIFICATION INFORMATION

(A) The ICA shall ensure that the following are lodged in the SMKI Repository:

(i) all IKI Certificates Issued by the IKI File Signing CA;

(ii) each version of this Policy; and

(iii) any other document or information that may from time to time be specified, for the purposes of this provision, by the SMKI PMA.

(B) The ICA may lodge in the SMKI Repository such other documents or information as it may from time to time consider appropriate.

2.3 TIME OR FREQUENCY OF PUBLICATION

(A) The ICA shall ensure that:

(i) each IKI Certificate Issued by the IKI File Signing CA is lodged in the SMKI Repository within 24 hours of its acceptance by a Subscriber; and

(ii) any other document that may from time to time be specified by the SMKI PMA is lodged in the SMKI Repository within such time as may be directed by the SMKI PMA.

2.4 ACCESS CONTROLS ON REPOSITORIES

(i) Provision in relation to access controls for the SMKI Repository is made in Sections L5.5, L5.6 and L5.6A of the Code.

3 IDENTIFICATION AND AUTHENTICATION

3.1 NAMING

3.1.1 Types of Names

(A) The ICA shall ensure that the IKI CPS contains provisions to ensure that the entity that is the Subject of each Certificate Issued to Eligible Subscribers is in accordance with the relevant Certificate Profile at Annex B.

3.1.2 Need for Names to be Meaningful

(A) The ICA shall ensure that the IKI CPS contains provisions to ensure that the name of the Subject of each IKI Certificate Issued to Eligible Subscribers is meaningful and consistent with the relevant Certificate Profile in Annex B.

3.1.3 Anonymity or Pseudonymity of Subscribers

(A) The ICA shall ensure that the IKI CPS contains provisions to:

(i) prohibit Eligible Subscribers from requesting the Issue of a Certificate anonymously or by means of a pseudonym; and

(ii) require the ICA to Authenticate Eligible Subscribers.

3.1.4 Rules for Interpreting Various Name Forms

(i) Provision in relation to name forms is made in Annex B.

3.1.5 Uniqueness of Names

(i) Provision in relation to the uniqueness of names is made in Annex B.

3.1.6 Recognition, Authentication, and Role of Trademarks

(i) Provision in relation to the use of trademarks, trade names and other restricted information in Certificates is made in Section L11 of the Code (Subscriber Obligations).

3.2 INITIAL IDENTITY VALIDATION

3.2.1 Method to Prove Possession of Private Key

(A) The ICA shall ensure that the IKI CPS contains provisions on:

(i) the procedure to be followed by an Eligible Subscriber in order to prove its possession of the Private Key which is associated with the Public Key contained in any Certificate that is the subject of a Certificate Signing Request; and

(ii) the procedure established for this purpose is in accordance with the procedure in PKCS#10.

3.2.2 Authentication of Organisation Identity

(A) Provision is made in the SMKI RAPP section 5.5 in relation to the:

(i) procedure to be followed by a Party, Manufacturer, RDP or SECCo in order to become an Authorised Subscriber;

(ii) criteria in accordance with which the ICA will determine whether a Party, Manufacturer, RDP or SECCo is entitled to become an Authorised Subscriber; and

(iii) requirement that the Party, Manufacturer, RDP or SECCo shall be Authenticated by the ICA for that purpose.

(B) Provision is made in the SMKI RAPP section 5 for the purpose of ensuring that the criteria in accordance with which the ICA shall Authenticate a Party, Manufacturer, RDP or SECCo shall be set to the level pursuant to the SMKI PMA Guidance on 'Verifying Organisation Identity' published on the Website.

3.2.3 Authentication of Individual Identity

(A) Provision is made in the SMKI RAPP in relation to the Authentication of persons engaged by Authorised Subscribers, which provides for all such persons to have their identity and authorisation verified to the level pursuant to the SMKI PMA Guidance on 'Verifying Individual Identity' published on the Website.

3.2.4 Non-verified Subscriber Information

(A) The ICA shall verify all information in relation to Certificates.

(B) Further provision on the content of ICA Certificates is made in Section L11 of the Code (Subscriber Obligations).

3.2.5 Validation of Authority

See Part 3.2.2 of this Policy.

3.2.6 Criteria for Interoperation

[Not applicable in this Policy]

3.3 IDENTIFICATION AND AUTHENTICATION FOR RE-KEY REQUESTS

3.3.1 Identification and Authentication for Routine Re-Key

(A) This Policy does not support Certificate Re-Key.

(B) The ICA shall not provide a Certificate Re-Key service.

3.3.2 Identification and Authentication for Re-Key after Revocation

[Not applicable in this Policy]

3.4 IDENTIFICATION AND AUTHENTICATION FOR REVOCATION REQUEST

3.4.1 Authentication for Certificate Revocation Requests

(A) Provision is made in the SMKI RAPP in relation to procedures designed to ensure the Authentication of persons who submit a Certificate Revocation Request and verify that they are authorised to submit that request.

4 CERTIFICATE AND LIFECYCLE OPERATIONAL REQUIREMENTS

4.1 CERTIFICATE APPLICATION

4.1.1 Submission of Certificate Applications

(A) Provision is made in the SMKI RAPP in relation to:

(i) in respect of an IKI Certificate:

(a) the circumstances in which a DCC RA Manager, DCC RA Personnel and ARO may submit a Certificate Signing Request; and

(b) the means by which it may do so, including through the use of an authorised System; and

(B) The ICA shall ensure that the IKI CPS contains provisions:

(i) in respect of an IKI Certificate:

(a) the circumstances in which Eligible Subscribers may submit a Certificate Signing Request; and

(b) the means by which it may do so, including through the use of an authorised System.

4.1.2 Enrolment Process and Responsibilities

(A) Provision is made in the SMKI RAPP sections 5 and 6 in relation to the:

(i) establishment of an enrolment process in respect of organisations, individuals and Systems in order to Authenticate them and verify that they are authorised to act on behalf of an Eligible Subscriber in its capacity as such; and

(ii) maintenance by the ICA of a list of organisations, individuals and Systems enrolled in accordance with that process.

4.1.3 Enrolment Process for the Registration Authority and its Representatives

(A) Provision is made in the SMKI RAPP section 6 in relation to the establishment of an enrolment process in respect of ICA Personnel and ICA Systems:

(i) in order to Authenticate them and verify that they are authorised to act on behalf of the ICA in its capacity as the Registration Authority; and

(ii) including in particular, for that purpose, provision:

(a) for the face-to-face or video link Authentication of all Registration Authority Personnel by a Registration Authority Manager; and

(b) for all Registration Authority Personnel to have their identify and authorisation verified to the level pursuant to the SMKI PMA Guidance on ‘Verifying Individual Identity’ published on the Website.

4.2 CERTIFICATE APPLICATION PROCESSING

4.2.1 Performing Identification and Authentication Functions

(A) Provision is made in the SMKI RAPP in relation to the Authentication by the ICA of DCC RA Managers, DCC RA Personnel and AROs which submit a Certificate Signing Request.

(B) The ICA shall ensure that the IKI CPS contains provisions in relation to the Authentication by the ICA of Eligible Subscribers which submit a Certificate Signing Request.

4.2.2 Approval or Rejection of Certificate Applications

(A) Where any Certificate Signing Request fails to satisfy the requirements set out in the SMKI RAPP, this Policy or any other provision of the Code, the ICA:

(i) shall reject it and refuse to Issue the Certificate which was the subject of the Certificate Signing Request; and

(ii) shall give notice to the Party, Manufacturer, RDP or SECCo which made the Certificate Signing Request of the reasons for its rejection.

(B) Where any Certificate Signing Request satisfies the requirements set out in the SMKI RAPP, this Policy or any other provision of the Code, the ICA shall Issue the Certificate which was the subject of the Certificate Signing Request.

4.2.3 Time to Process Certificate Applications

(A) The ICA shall ensure that it processes all Certificate Signing Requests relating to IKI Certificates promptly, and in any event in accordance with such time as is specified in the SMKI RAPP.

4.3 CERTIFICATE ISSUANCE

4.3.1 ICA Actions during Certificate Issuance

(A) The ICA may Issue a Certificate only:

(i) in accordance with the provisions of this Policy; and

(ii) in response to a Certificate Signing Request made by an Eligible Subscriber in accordance with this Policy.

(B) The ICA shall ensure that:

(i) each ICA Certificate Issued by it contains information that it has verified to be correct and complete; and

(ii) each IKI Certificate Issued by it contains information consistent with the information in the Certificate Signing Request.

(C) An ICA Certificate may only be:

(i) Issued by the ICA; and

(ii) for that purpose, signed using the Root ICA Private Key.

(D) An IKI Certificate may only be:

(i) Issued by the ICA; and

(ii) for that purpose, signed using an Issuing ICA Private Key.

(E) The ICA shall not Issue:

(i) an Issuing ICA Certificate using a Root ICA Private Key after the expiry of the Validity Period of a Root ICA Certificate containing the Public Key associated with that Private Key; or

(ii) an IKI Certificate using an Issuing ICA Private Key after the expiry of the Validity Period of an Issuing ICA Certificate containing the Public Key associated with that Private Key.

4.3.2 Notification to Eligible Subscriber by the ICA of Issuance of Certificate

(A) Provision is made in the SMKI RAPP for the ICA to notify DCC RA Manager, DCC RA Personnel and ARO where that DCC RA Manager, DCC RA Personnel or AROs is Issued with a Certificate which was the subject of a Certificate Signing Request made by them.

(B) The ICA shall ensure the IKI CPS includes provisions for the ICA to notify Eligible Subscribers where that Eligible Subscriber is Issued with a Certificate which was the subject of a Certificate Signing Request made by them.

4.4 CERTIFICATE ACCEPTANCE

4.4.1 Conduct Constituting Certificate Acceptance

(A) Provision is made in the SMKI RAPP to:

(i) specify a means by which the Eligible Subscriber may clearly indicate to the ICA its rejection of a Certificate which has been Issued to it; and

(ii) ensure that the Eligible Subscriber to which a Certificate has been Issued, and which has not been rejected, is treated as having accepted that Certificate.

(B) A Certificate which has been Issued by the ICA shall not be treated as valid for any purposes of this Policy or the Code until it is treated as having been accepted by the Eligible Subscriber to which it was Issued.

(C) The ICA shall maintain a record of all Certificates which have been Issued by it and are treated as accepted by a Subscriber.

(D) Further provision in relation to the rejection and acceptance of Certificates is made in Section L11.7 of the Code.

4.4.2 Publication of Certificates by the ICA

(A) Provision in relation to the publication of Certificates is made in Part 2 of this Policy.

4.4.3 Notification of Certificate Issuance by the ICA to Other Entities

(A) The ICA shall give notice of the Issue of a Certificate only to the Eligible Subscriber which submitted a Certificate Signing Request in respect of that Certificate.

4.5 KEY PAIR AND CERTIFICATE USAGE

4.5.1 Subscriber Private Key and Certificate Usage

(A) Provision for restrictions on the use by Subscribers of Private Keys in respect of Certificates is made in:

(i) Section L11.8 of the Code; and

(ii) this Policy.

4.5.2 Relying Party Public Key and Certificate Usage

(A) Provision in relation to reliance that may be placed on a Certificate is made in Section L12 of the Code (Relying Party Obligations).

4.6 CERTIFICATE RENEWAL

4.6.1 Circumstances of Certificate Renewal

(A) This Policy does not support the renewal of Certificates.

(B) The ICA may only replace, and shall not renew, any Certificate.

4.6.2 Circumstances of Certificate Replacement

(A) Where any ICA System or any ICA Private Key is (or is suspected by the ICA of being) Compromised, the ICA shall:

(i) immediately notify the SMKI PMA;

(ii) provide the SMKI PMA with all of the information known to it in relation to the nature and circumstances of the event of Compromise or suspected Compromise; and

(iii) where the Compromise or suspected Compromise relates to an ICA Private Key:

(a) ensure that the Private Key is no longer used;

(b) promptly notify each of the Subscribers for any IKI Certificates Issued using that Private Key; and

(c) promptly notify the SMKI PMA, verifiably destroy the ICA Private Key Material and revoke the corresponding ICA Certificate.

(B) Where the ICA Root Private Key is Compromised (or is suspected by the ICA of being Compromised), the ICA:

(i) may issue a replacement for any ICA Certificate that has been Issued using that Private Key; and

(ii) shall ensure that the Subscriber for that ICA Certificate both applies for the Issue of a new Certificate in accordance with this Policy and revokes that ICA Certificate.

(C) The ICA shall ensure that a replacement for each ICA Certificate is Issued prior to end of the Validity Period of that ICA Certificate.

(D) A Subscriber for an IKI Certificate may request a replacement for that Certificate at any time by applying for the Issue of a new IKI Certificate in accordance with this Policy and, where this replacement is for purposes other than to replace an expiring Certificate, shall submit a Certificate Revocation Request in respect of the replaced IKI Certificate.

4.6.3 Who May Request a Replacement Certificate

See Part 4.1 of this Policy.

4.6.4 Processing Replacement Certificate Requests

See Part 4.2 of this Policy.

4.6.5 Notification of Replacement Certificate Issuance to a Subscriber

See Part 4.3.2 of this Policy.

4.6.6 Conduct Constituting Acceptance of a Replacement Certificate

See Part 4.4.1 of this Policy.

4.6.7 Publication of a Replacement Certificate by the ICA

[Not applicable in this Policy]

4.6.8 Notification of Certificate Issuance by the ICA to Other Entities

[Not applicable in this Policy]

4.7 CERTIFICATE RE-KEY

4.7.1 Circumstances for Certificate Re-Key

(A) This Policy does not support Certificate Re-Key.

(B) The ICA shall not provide a Certificate Re-Key service.

(C) Where a new Key Pair has been generated, the Subscriber shall apply for a new Certificate in accordance with this Policy.

4.7.2 Who may Request Certification of a New Public Key

[Not applicable to this Policy]

4.7.3 Processing Certificate Re-Keying Requests

[Not applicable to this Policy]

4.7.4 Notification of New Certificate Issuance to Subscriber

[Not applicable to this Policy]

4.7.5 Conduct Constituting Acceptance of a Re-Keyed Certificate

[Not applicable to this Policy]

4.7.6 Publication of the Re-Keyed Certificate by the ICA

[Not applicable to this Policy]

4.7.7 Notification of Certificate Issuance by the ICA to Other Entities

[Not applicable to this Policy]

4.8 CERTIFICATE MODIFICATION

4.8.1 Circumstances for Certificate Modification

(A) This Policy does not support Certificate modification.

(B) Neither the ICA nor any Subscriber may modify a Certificate.

4.8.2 Who may request Certificate Modification

[Not applicable to this Policy]

4.8.3 Processing Certificate Modification Requests

[Not applicable to this Policy]

4.8.4 Notification of New Certificate Issuance to Subscriber

[Not applicable to this Policy]

4.8.5 Conduct Constituting Acceptance of Modified Certificate

[Not applicable to this Policy]

4.8.6 Publication of the Modified Certificate by the ICA

[Not applicable to this Policy]

4.8.7 Notification of Certificate Issuance by the ICA to Other Entities

[Not applicable to this Policy]

4.9 CERTIFICATE REVOCATION AND SUSPENSION

4.9.1 Circumstances for Revocation

(A) A Subscriber shall ensure that it submits a Certificate Revocation Request in relation to a Certificate:

(i) immediately upon becoming aware that the Certificate has been Compromised, or is suspected of having been Compromised, due to the Compromise of the Private Key associated with the Public Key contained within that Certificate;

(ii) when any of the permitted reasons for revocation of authentication credentials, as set out in the SMKI RAPP, are met; or

(iii) immediately upon ceasing to be an Eligible Subscriber in respect of that Certificate; provided that, where a Supplier of Last Resort has been appointed in relation to premises supplied by the Subscriber, the Subscriber shall not submit a Certificate Revocation Request.

(B) The ICA must revoke a Certificate upon:

(i) receiving a Certificate Revocation Request if the Certificate to which that request relates has been Authenticated in accordance with Part 3.4.1 of this Policy; or

(ii) being directed to do so by the SMKI PMA.

(C) The ICA must revoke a Certificate in relation to which it has not received a Certificate Revocation Request:

(i) where it becomes aware that the Certificate has been Compromised, or is suspected of having been Compromised, due to the Compromise of the Private Key associated with the Public Key contained within that Certificate; or

(ii) (subject to the Section L16.1 (Supplier of Last Resort) of the Code) where it becomes aware that the Subscriber for that Certificate has ceased to be an Eligible Subscriber in respect of the Certificate.

(D) In an extreme case, where it considers it necessary to do so for the purpose of preserving the integrity of the SMKI Services, the ICA may, on the receipt of a Certificate Revocation Request in relation to a Certificate which has not been Authenticated in accordance with Part 3.4.1 of this Policy, revoke that Certificate.

(E) Where the ICA revokes a Certificate in accordance with paragraph (D) it shall notify the SMKI PMA and provide a statement of its reasons for the revocation.

4.9.2 Who can Request Revocation

(A) Any Subscriber may submit a Certificate Revocation Request in relation to a Certificate for which it is the Subscriber, and shall on doing so:

(i) provide all the information specified in the SMKI RAPP (including all the information necessary for the Authentication of the Certificate); and

(ii) specify its reason for submitting the Certificate Revocation Request (which shall be a reason consistent with Part 4.9.1(A) of this Policy).

(B) The SMKI PMA may direct the ICA to revoke a Certificate.

(C) The ICA may elect to revoke a Certificate in accordance with Part 4.9.1(D) of this Policy.

4.9.3 Procedure for Revocation Request

(A) Provision is made in the SMKI RAPP in relation to the procedure for submitting and processing a Certificate Revocation Request associated with Certificates Issued to DCC Registration Authority (RA) Managers, DCC RA Personnel, Authorised Responsible Officers (AROs).

(B) The ICA shall ensure that the IKI CPS contains provisions in relation to the procedure for submitting and processing a Certificate Revocation Request associated with Certificates Issued to Eligible Subscribers.

(C) On receiving a Certificate Revocation Request, the ICA shall use its reasonable steps to:

(i) Authenticate the Subscriber making that request;

(ii) Authenticate the Certificate to which the request relates; and

(iii) confirm that a reason for the request has been specified in accordance with Part 4.9.2 of this Policy.

(D) Where the ICA, in accordance with Part 4.9.1(C) of this Policy, intends to revoke a Certificate in relation to which it has not received a Certificate Revocation Request, it shall use its best steps prior to revocation to confirm with the Subscriber for that Certificate the circumstances giving rise to the revocation.

(E) The ICA shall inform the Subscriber for a Certificate where that Certificate has been revoked.

4.9.4 Revocation Request Grace Period

[Not applicable in this Policy]

4.9.5 Time within which ICA must process the Revocation Request

(A) The ICA shall ensure that it processes all Certificate Revocation Requests as soon as reasonably practicable, and in any event in accordance with such time as is specified in the SMKI RAPP.

4.9.6 Revocation Checking Requirements for Relying Parties

(A) Provision in relation to the revocation checking requirements for Relying Parties is made in Section L12.3 of the Code.

4.9.7 CRL Issuance Frequency (if applicable)

(A) The ICA shall ensure that an up to date version of the IKI ARL is made available to Relying Parties set out in 1.3.5(E) of this Policy.

(i) at least once in every period of twelve months; and

(ii) promptly on the revocation of an ICA Certificate.

(B) Each version of the IKI ARL shall be valid until the date which is 12 months after the date on which that version of the IKI ARL is produced.

(C) Further provision in relation to the reliance that may be placed on the IKI ARL (and on versions of it) is set out in Section L12 of the Code (Relying Party Obligations).

(D) The ICA shall ensure that an up to date version of the IKI CRL is made available to Relying Parties set out in 1.3.5(E) of this Policy:

(i) at least once in every period of twelve hours; and

(ii) within one hour on the revocation of an IKI Certificate.

(E) Each version of the IKI CRL shall be valid until 48 hours from the time at which it is produced. (F) Further provision in relation to the reliance that may be placed on the IKI CRL (and on versions of it) is set out in Section L12 of the Code (Relying Party Obligations).

(G) The ICA shall ensure that each up to date version of the IKI ARL and IKI CRL:

(i) continues to include each relevant revoked Certificate until such time as the Validity Period of that Certificate has expired; and

(ii) does not include any revoked Certificate after the Validity Period of that Certificate has expired.

(H) The ICA shall ensure that the IKI CRL contains a non-critical entry extension which identifies the reason for the revocation of each Certificate listed on it in accordance with RFC 5280 (section 5.3.1).

(I) The ICA shall retain a copy of the information contained in all versions of the IKI CRL and IKI ARL, together with the dates and times between which each such version was valid. This information shall be made available as soon as is reasonably practicable, on receipt of a request, to the Panel, the SMKI PMA, any Subscriber or any Relying Party.

4.9.8 Maximum Latency for CRLs (if applicable)

See Part 4.9.7 of this Policy.

4.9.9 On-line Revocation/Status Checking Availability

(A) This Policy supports on-line revocation status checking.

(B) The ICA shall provide on-line revocation status checking service.

4.9.10 On-line Revocation Checking Requirements

[Not applicable in this Policy]

4.9.11 Other Forms of Revocation Advertisements Available

[Not applicable in this Policy]

4.9.12 Special Requirements in the Event of Key Compromise

See Part 4.6.2 of this Policy.

4.9.13 Circumstances for Suspension

[Not applicable in this Policy]

4.9.14 Who can Request Suspension

[Not applicable in this Policy]

4.9.15 Procedure for Suspension Request

[Not applicable in this Policy]

4.9.16 Limits on Suspension Period

[Not applicable in this Policy]

4.10 CERTIFICATE STATUS SERVICES

4.10.1 Operational Characteristics

[Not applicable in this Policy]

4.10.2 Service Availability

(A) In circumstances in which:

(i) an up to date version of the IKI ARL has not been made available to the DCC in accordance with Part 4.9.7(A) of this Policy,

the DCC shall be entitled to rely on the IKI ARL for the period during which it remains valid in accordance with the provisions of Part 4.9.7(B) of this Policy, but thereafter shall not rely on any Certificate.

(B) In circumstances in which:

(i) an up to date version of the IKI CRL has not been made available to the DCC in accordance with Part 4.9.7(C) of this Policy

the DCC shall be entitled to rely on the IKI CRL for the period during which it remains valid in accordance with the provisions of Part 4.9.7(D) of this Policy, but thereafter shall not rely on any IKI Certificate.

4.10.3 Optional Features

[Not applicable in this Policy]

4.11 END OF SUBSCRIPTION

[Not applicable in this Policy]

4.12 KEY ESCROW AND RECOVERY

4.12.1 Key Escrow and Recovery Policies and Practices

(A) This Policy does not support Key Escrow.

(B) The ICA shall not provide any Key Escrow service.

4.12.2 Session Key Encapsulation and Recovery Policy and Practices

[Not applicable in this Policy]

5 FACILITY MANAGEMENT AND OPERATIONAL CONTROLS

5.1 PHYSICAL CONTROLS

5.1.1 Site Location and Construction

(A) The ICA shall ensure that the ICA Systems are operated in a sufficiently secure environment, which shall at least satisfy the requirements set out at Section G2 (System Security: Obligations on the DCC) and Section G5 (Information Security: Obligations on the DCC and Users) of the Code.

(B) The ICA shall ensure that:

(i) all of the physical locations in which the ICA Systems are situated, operated, routed or directly accessed are in the United Kingdom;

(ii) all bespoke Security Related Functionality is developed, specified, designed, built and tested only within the United Kingdom; and

(iii) all Security Related Functionality is integrated, configured, tested in situ, implemented, operated and maintained only within the United Kingdom.

(C) The ICA shall ensure that the ICA Systems cannot be indirectly accessed from any location outside the United Kingdom.

(D) The ICA shall ensure that the IKI CPS incorporates provisions designed to ensure that all physical locations in which the manufacture of Certificates and Time-Stamping take place are at all times manually or electronically monitored for unauthorised intrusion in accordance with SMKI PMA Guidance on ‘Protective Monitoring’ published on the Website.

(E) The ICA shall ensure that the IKI CPS incorporates provisions designed to ensure that all PINs, pass-phrases and passwords used for the purposes of carrying out the functions of the ICA are stored in secure containers accessible only to appropriately authorised individuals.

(F) The ICA shall ensure that the ICA Systems are Separated from any DCA or OCA Systems, save that any Systems used for the purposes of the Registration Authority functions of the ICA and DCA or OCA shall not require to be Separated.

5.1.2 Physical Access

(A) The ICA shall ensure that the IKI CPS incorporates provisions in relation to access control, including in particular provisions designed to:

(i) establish controls such that only appropriately authorised personnel may have unescorted physical access to ICA Systems or any System used for the purposes of Time-Stamping;

(ii) ensure that any unauthorised personnel may have physical access to such Systems only if appropriately authorised and supervised;

(iii) ensure that a site access log is both maintained and periodically inspected for all locations at which such Systems are sited; and

(iv) ensure that all removable media which contain sensitive plain text Data and are kept at such locations are stored in secure containers accessible only to appropriately authorised individuals.

5.1.3 Power and Air Conditioning

(A) The ICA shall ensure that the IKI CPS incorporates provisions in relation to power and air conditioning at all physical locations in which the ICA Systems are situated.

5.1.4 Water Exposure

(A) The ICA shall ensure that the IKI CPS incorporates provisions in relation to water exposure at all physical locations in which the ICA Systems are situated.

5.1.5 Fire Prevention and Protection

(A) The ICA shall ensure that the IKI CPS incorporates provisions in relation to fire prevention and protection at all physical locations in which the ICA Systems are situated.

5.1.6 Media Storage

(A) The ICA shall ensure that the IKI CPS incorporates provisions designed to ensure that appropriate controls are placed on all media used for the storage of Data held by it for the purposes of carrying out its functions as the ICA.

5.1.7 Waste Disposal

(A) The ICA shall ensure that all media used to store Data held by it for the purposes of carrying out its functions as the ICA are disposed of only using secure methods of disposal in accordance with https://www.ncsc.gov.uk/guidance/secure-sanitisation-storage-media.

5.1.8 Off-Site Back-Up

(A) The ICA shall regularly carry out a Back-Up of:

(i) all Data held on the ICA Systems which are critical to the operation of those Systems or continuity in the provision of the SMKI Services; and

(ii) all other sensitive Data.

(B) For the purposes of paragraph (A), the ICA shall ensure that the IKI CPS incorporates provisions which identify the categories of critical and sensitive Data that are to be Backed-Up.

(C) The ICA shall ensure that Data which are Backed-Up in accordance with paragraph (A):

(i) are stored on media that are located in physically secure facilities in different locations to the sites at which the Data being Backed-Up are ordinarily held;

(ii) are protected in accordance with the outcome of a risk assessment which is documented in the IKI CPS, including when being transmitted for the purposes of Back-Up; and

(iii) to the extent to which they comprise ICA Private Key Material, are Backed-Up:

(a) using the proprietary Back-Up mechanisms specific to the relevant Cryptographic Module; and

(b) in a manner that is compliant with FIPS 140-2 Level 3 (or any equivalent to that Federal Information Processing Standard which updates or replaces it from time to time).

(D) The ICA shall ensure that, where any elements of the ICA Systems, any Data held for the purposes of providing the SMKI Services, or any items of ICA equipment are removed from their primary location, they continue to be protected in accordance with the security standard appropriate to the primary location.

5.2 PROCEDURAL CONTROLS

5.2.1 Trusted Roles

(A) The ICA shall ensure that:

(i) no individual may carry out any activity which involves access to resources, or Data held on, the ICA Systems unless that individual has been expressly authorised to have such access;

(ii) each member of ICA Personnel has a clearly defined level of access to the ICA Systems and the premises in which they are located;

(iii) no individual member of ICA Personnel is capable, by acting alone, of engaging in any action by means of which the ICA Systems may be Compromised to a material extent; and

(iv) the IKI CPS incorporates provisions designed to ensure that appropriate controls are in place for the purposes of compliance by the ICA with the requirements of this paragraph.

5.2.2 Number of Persons Required per Task

(A) The ICA shall ensure that the IKI CPS incorporates provisions designed to establish:

(i) the appropriate separation of roles between the different members of ICA Personnel; and

(ii) the application of controls to the actions of all members of ICA Personnel who are Privileged Persons, in particular:

(a) identifying any controls designed to ensure that the involvement of more than one individual is required for the performance of certain functions; and

(b) providing that the revocation of any ICA Certificate is one such function.

(B) The ICA shall ensure that the IKI CPS, as a minimum, makes provision for the purposes of paragraph (A) in relation to the following roles:

(i) ICA Systems administration;

(ii) ICA Systems operations;

(iii) ICA Systems security; and

(iv) ICA Systems auditing.

5.2.3 Identification and Authentication for Each Role

See Part 5.2.2 of this Policy.

5.2.4 Roles Requiring Separation of Duties

See Part 5.2.2 of this Policy.

5.3 PERSONNEL CONTROLS

5.3.1 Qualification, Experience and Clearance Requirements

(A) The ICA shall ensure that all ICA Personnel must:

(i) be appointed to their roles in writing;

(ii) be bound by contract to the terms and conditions relevant to their roles;

(iii) have received appropriate training with respect to their duties;

(iv) be bound by contract not to disclose any confidential, sensitive, personal or security-related Data except to the extent necessary for the performance of their duties or for the purposes of complying with any requirement of law; and

(v) in so far as can reasonably be ascertained by the ICA, not have been previously relieved of any past assignment (whether for the ICA or any other person) on the grounds of negligence or any other failure to perform a duty.

(B) The ICA shall ensure that all ICA Personnel have, as a minimum, passed a Security Check before commencing their roles.

5.3.2 Background Check Procedures

See Part 5.3.1 of this Policy.

5.3.3 Training Requirements

See Part 5.3.1 of this Policy.

5.3.4 Retraining Frequency and Requirements

(A) The ICA shall ensure that the IKI CPS incorporates appropriate provisions relating to the frequency and content of retraining and refresher training to be undertaken by members of ICA Personnel.

5.3.5 Job Rotation Frequency and Sequence

(A) The ICA shall ensure that the IKI CPS incorporates appropriate provisions relating to the frequency and sequence of job rotations to be undertaken by members of ICA Personnel.

5.3.6 Sanctions for Unauthorised Actions

(A) The ICA shall ensure that the IKI CPS incorporates appropriate provisions relating to sanctions for unauthorised actions undertaken by members of ICA Personnel.

5.3.7 Independent Contractor Requirements

(A) In accordance with the provisions of the Code, references to the ICA in this Policy include references to persons with whom the ICA contracts in order to secure performance of its obligations as the ICA.

5.3.8 Documentation Supplied to Personnel

(A) The ICA shall ensure that all ICA Personnel are provided with access to all documents relevant to their roles or necessary for the performance of their duties, including in particular:

(i) this Policy;

(ii) the IKI CPS; and

(iii) any supporting documentation, statutes, policies or contracts.

5.4 AUDIT LOGGING PROCEDURES

5.4.1 Types of Events Recorded

(A) The ICA shall ensure that:

(i) the ICA Systems record all systems activity in an audit log;

(ii) the IKI CPS incorporates a comprehensive list of all events that are to be recorded in an audit log in relation to:

(a) the activities of ICA Personnel;

(b) the use of ICA equipment;

(c) the use of (including both authorised and unauthorised access, and attempted access to) any premises at which functions of the ICA are carried out;

(d) communications and activities that are related to the Issue of Certificates (in so far as not captured by the ICA Systems audit log); and

(iii) it records in an audit log all the events specified in paragraph (ii).

5.4.2 Frequency of Processing Log

(A) The ICA shall ensure that:

(i) the audit logging functionality in the ICA Systems is fully enabled at all times;

(ii) all ICA Systems activity recorded in the Audit Log is recorded in a standard format that is compliant with:

(a) British Standard BS 10008:2014 (Evidential Weight and Legal Admissibility of Electronic Information); or

(b) any equivalent to that British Standard which updates or replaces it from time to time; and

(iii) it monitors the ICA Systems in compliance with the SMKI PMA Guidance on “Protective Monitoring” published on the Website.

;

(B) The ICA shall ensure that the IKI CPS incorporates provisions which specify:

(i) how regularly information recorded in the Audit Log is to be reviewed; and

(ii) what actions are to be taken by it in response to types of events recorded in the Audit Log.

(C) The ICA shall ensure that the IKI CPS incorporates provisions in relation to access to the Audit Log, providing in particular that:

(i) Data contained in the Audit Log must not be accessible other than on a read-only basis; and

(ii) access to those Data must be limited to those members of ICA Personnel who are performing a dedicated system audit role.

5.4.3 Retention Period for Audit Log

(A) The ICA shall:

(i) retain the Audit Log so that it incorporates, on any given date, a record of all system events occurring during a period of at least twelve months prior to that date; and

(ii) ensure that a copy of the Audit Log incorporating a record of all system events occurring prior to the beginning of that period is archived in accordance with the requirements of Part 5.5 of this Policy.

5.4.4 Protection of Audit Log

(A) The ICA shall ensure that:

(i) to the extent to which the Audit Log is retained electronically, the Data stored in it cannot be accessed other than on a read-only basis, and are protected from unauthorised viewing, modification and deletion in accordance with:

(a) British Standard BS 10008:2014 (Evidential Weight and Legal Admissibility of Electronic Information); or

(b) any equivalent to that British Standard which updates or replaces it from time to time; and

(ii) to the extent to which the Audit Log is retained in non-electronic form, the Data stored in it are appropriately protected from unauthorised viewing, modification and destruction in order to ensure that their integrity is maintained for evidential purposes.

5.4.5 Audit Log Back-Up Procedures

(A) The ICA shall ensure that the Data contained in the Audit Log are Backed-Up (or, to the extent that the Audit Log is retained in non-electronic form, are copied):

(i) on a daily basis; or

(ii) if activity has taken place on the ICA Systems only infrequently, in accordance with the schedule for the regular Back-Up of the Data held on those Systems.

(B) The ICA shall ensure that all Data contained in the Audit Log which are Backed-Up are, during Back-Up:

(i) held in accordance with the outcome of a risk assessment which is documented in the IKI CPS; and

(ii) protected to the same standard of protection as the primary copy of the Audit Log in accordance with Part 5.4.4 of this Policy.

5.4.6 Audit Collection System (Internal or External)

(A) The ICA shall ensure that the IKI CPS incorporates provisions in relation to its system for collecting Data for the purpose of populating the Audit Log.

5.4.7 Notification to Event-Causing Subject

(A) The ICA shall ensure that the IKI CPS incorporates provisions in relation to its notification of any person who is (or is responsible for any System which is) the direct cause of an event recorded in the Audit Log.

5.4.8 Vulnerability Assessments

(A) Provision is made in Sections G2.13 to G2.14 of the Code (Management of Vulnerabilities) in relation to the carrying out of vulnerability assessments in respect of the ICA Systems.

5.5 RECORDS ARCHIVAL

5.5.1 Types of Records Archived

(A) The ICA shall ensure that it archives:

(i) the Audit Log in accordance with Part 5.4.3 of this Policy;

(ii) its records of all Data submitted to it by Eligible Subscribers for the purposes of Certificate Signing Requests; and

(iii) any other Data specified in this Policy or the Code as requiring to be archived in accordance with this Part 5.5.

5.5.2 Retention Period for Archive

(A) The ICA shall ensure that all Data which are Archived are retained for a period of at least seven years from the date on which they were Archived.

5.5.3 Protection of Archive

(A) The ICA shall ensure that Data held in its Archive are:

(i) protected against any unauthorised access;

(ii) adequately protected against environmental threats such as temperature, humidity and magnetism; and

(iii) incapable of being modified or deleted.

5.5.4 Archive Back-Up Procedures

(A) The ICA shall ensure that the IKI CPS incorporates provisions in relation to its procedures for the Back-Up of its Archive.

5.5.5 Requirements for Time-Stamping of Records

(A) Provision in relation to Time-Stamping is made in Part 6.8 of this Policy.

5.5.6 Archive Collection System (Internal or External)

(A) The ICA shall ensure that the IKI CPS incorporates provisions in relation to its system for collecting Data for the purpose of populating the Archive.

5.5.7 Procedures to Obtain and Verify Archive Information

(A) The ICA shall ensure that:

(i) Data held in the Archive are stored in a readable format during their retention period; and

(ii) those Data remains accessible at all times during their retention period, including during any period of interruption, suspension or cessation of the ICA’s operations.

(B) The ICA shall ensure that the IKI CPS incorporates provisions in relation to the periodic verification by the ICA of the Data held in the Archive.

5.6 KEY CHANGEOVER

5.6.1 IKI Certificate Key Changeover

(A) The ICA shall Issue a new IKI Certificate in relation to a Subject where a new Certificate Signing Request is submitted by an Eligible Subscriber in accordance with the requirements of the SMKI RAPP and this Policy.

5.6.2 ICA Key Changeover

(A) Where the ICA ceases to use an ICA Private Key in accordance with the requirements of Part 4.3.1(E) of this Policy, it shall:

(i) either:

(a) verifiably destroy the ICA Private Key Material; or

(b) retain the ICA Private Key Material in such a manner that it is adequately protected against being put back into use;

(ii) generate a new Key Pair;

(iii) ensure that any relevant Certificate subsequently Issued by it is Issued using the ICA Private Key from the newly-generated Key Pair:

(a) until the time determined in accordance with Part 4.3.1(E) of this Policy; and

(b) subject to the provisions of Part 5.7.1(C) of this Policy; and

(iv) in its capacity as the Root ICA Issue a new relevant ICA Certificate.

(B) The ICA shall ensure that the actions taken by it in accordance with the requirements of paragraph (A) are managed so as to prevent any disruption to the provision of the SMKI Services.

5.6.3 Subscriber Key Changeover

(A) Where:

(i) a Certificate has been revoked in accordance with Part 4.9 of this Policy; and

(ii) the Subscriber for that Certificate submits to the ICA a Certificate Signing Request for the Issue of a replacement Certificate,

the ICA shall verify that the reasons for the revocation and replacement of the previous Certificate have been satisfactorily addressed, and may Issue a Certificate in accordance with the Certificate Signing Request only after it has done so.

5.7 COMPROMISE AND DISASTER RECOVERY

5.7.1 Incident and Compromise Handling Procedures

(A) The ICA shall ensure that the IKI CPS incorporates a business continuity plan which shall be designed to ensure:

(i) continuity in, or (where there has been unavoidable discontinuity) the recovery of, the provision of the SMKI Services in the event of any Compromise of the ICA Systems or major failure in the ICA processes; and

(ii) that priority is given to maintain continuity in, or to recovering the capacity for, the revocation of Certificates and the making available of an up to date IKI ARL and IKI CRL.

(B) The ICA shall ensure that the procedures set out in the business continuity plan are:

(i) compliant with ISO 22301 and ISO 27031 (or any equivalent to those standards which update or replace them from time to time); and

(ii) tested periodically, and in any event at least once in each year, in order to ensure that they are operationally effective.

(C) The ICA shall ensure that the IKI CPS incorporates provisions setting out the approach to be taken by it in circumstances in which it suspects (or has reason to suspect) that any ICA Private Key or any part of the ICA Systems is Compromised.

5.7.2 Computing Resources, Software and/or Data are Corrupted

(A) The ICA shall ensure that the business continuity plan established in accordance with Part 5.7.1 of this Policy incorporates provisions setting out the steps to be taken in the event of any loss of or corruption to computing resources, software or Data.

5.7.3 Entity Private Key Compromise Procedures

See Part 5.7.1 of this Policy.

5.7.4 Business Continuity Capabilities after a Disaster

(A) The ICA shall ensure that the business continuity plan established in accordance with Part 5.7.1 of this Policy is designed to ensure the recovery of the provision of the SMKI Services within not more than 12 hours of the occurrence of any event causing discontinuity.

5.8 CERTIFICATION AUTHORITY AND REGISTRATION AUTHORITY TERMINATION

[Not applicable in this Policy]

6 TECHNICAL SECURITY CONTROLS

The ICA shall ensure that the IKI CPS incorporates detailed provision in relation to the technical controls to be established and operated for the purposes of the exercise of its functions as the Root ICA the Issuing ICA and the Registration Authority.

6.1 KEY PAIR GENERATION AND INSTALLATION

6.1.1 Key Pair Generation

(A) The ICA shall ensure that all ICA Keys are generated:

(i) in a protected environment compliant with FIPS 140-2 Level 3 (or any equivalent to that Federal Information Processing Standard which updates or replaces it from time to time);

(ii) using multi-person control, such that no single Privileged Person is capable of generating any ICA Key; and

(iii) using random numbers of such length as to make it computationally infeasible to regenerate them even with knowledge of when and by means of which equipment they were generated.

(B) The ICA shall not generate any Private Key or Public Key other than an ICA Key.

6.1.2 Private Key Delivery to Subscriber

(A) In accordance with Part 6.1.1(B), the ICA shall not generate any Private Key for delivery to a Subscriber.

6.1.3 Public Key Delivery to Certificate Issuer

(A) The ICA shall ensure that the IKI CPS incorporates provisions:

(i) in relation to the mechanism by which Public Keys of Subscribers are delivered to it for the purpose of the exercise of its functions as the Root ICA and Issuing ICA; and

(ii) ensuring that the mechanism uses a recognised standard protocol such as PKCS#10.

6.1.4 ICA Public Key Delivery to Relying Parties

(A) The ICA shall ensure that the IKI CPS incorporates provisions:

(i) in relation to the manner by which each IKI Certificate Issued by the IKI File Signing CA is made available to Relying Parties;

(ii) designed to ensure that the IKI Certificates Issued by the IKI File Signing CA are made available to Relying Parties in such a manner as to guarantee that their integrity is maintained.

6.1.5 Key Sizes

(A) The ICA and every Subscriber shall ensure that all Private Keys and Public Keys which each of them may use for the purposes of this Policy are of the following size and characteristics

(i) 4096-bit RSA for the Root Certificate, or 2048-bit RSA for all subordinate Certificates including the Issuing ICA Certificate; and

(ii) SHA256-with-RSA Encryption as specified in RFC 4055.

6.1.6 Public Key Parameters Generation and Quality Checking

(A) The ICA shall ensure that any Public Key used by it for the purposes of this Policy shall be of values and lengths that make the success of known attacks infeasible.

(B) Each Subscriber shall ensure that any Public Key used by it for the purposes of this Policy shall be of values and lengths that make the success of known attacks infeasible.

6.1.7 Key Usage Purposes (as per X.509 v3 Key Usage Field)

(A) The ICA shall ensure that each Certificate that is Issued by it has a 'keyUsage' field in accordance with RFC 5280.

(B) The ICA shall ensure that each IKI Certificate that is Issued by it has a 'keyUsage' of 'digitalSignature'.

(C) The ICA shall ensure that each ICA Certificate that is Issued by it has a 'keyUsage' of either:

(i) 'keyCertSign'; or

(ii) 'CRLSign'.

(D) The ICA shall ensure that no 'keyUsage' values may be set in an IKI Certificate or ICA Certificate other than in accordance with this Part 6.1.7.

6.1.8 Extended Key Usage Purposes

(A) The ICA shall ensure that each Certificate that is Issued by the IKI Administrator CA, IKI Authorised Device Subscriber CA, IKI Authorised Organisation Subscriber CA, IKI Authorised Internet Organisation Subscriber CA, IKI Authorised Web Service Subscriber CA and IKI Registration Authority CA has an 'extendedkeyUsage' field in accordance with RFC 5280.

(B) The ICA shall ensure that each IKI Certificate that is Issued by the IKI Administrator CA, IKI Authorised Device Subscriber CA, IKI Authorised Organisation Subscriber CA, IKI Authorised Internet Organisation Subscriber CA, IKI Authorised Web Service Subscriber CA and IKI Registration Authority CA has an 'extendedKeyUsage' set to 'clientAuth'.

6.2 PRIVATE KEY PROTECTION AND CRYPTOGRAPHIC MODULE ENGINEERING CONTROLS

6.2.1 Cryptographic Module Standards and Controls

(A) The ICA shall ensure that all ICA Private Keys shall be:

(i) protected to a high standard of assurance by physical and logical security controls; and

(ii) stored in and operated from within a Cryptographic Module which is compliant with FIPS 140-2 Level 3 (or any equivalent to that Federal Information Processing Standard which updates or replaces it from time to time).

(B) The ICA shall ensure that all ICA Private Keys shall, where they affect the outcome of any Certificates Issued by it, be protected by, stored in and operated from within a Cryptographic Module which is compliant with FIPS 140-2 Level 3 (or any equivalent to that Federal Information Processing Standard which updates or replaces it from time to time).

(C) The ICA shall ensure that no ICA Private Key shall be made available in either complete or unencrypted form except in a Cryptographic Module which is compliant with FIPS 140-2 Level 3 (or any equivalent to that Federal Information Processing Standard which updates or replaces it from time to time).

(D) The ICA shall ensure that any Cryptographic Module which is used for any purpose related to Certificate life-cycle management shall:

(i) operate so as to block access to itself following a number of failed consecutive attempts to access it using Activation Data, where that number shall be set out in the IKI CPS; and

(ii) be required to be unblocked by an authorised member of ICA Personnel who has been Authenticated as such following a process which shall be set out in the IKI CPS.

6.2.2 Private Key (m out of n) Multi-Person Control

See Part 6.1.1 of this Policy.

6.2.3 Private Key Escrow

(A) This Policy does not support Key Escrow.

(B) The ICA shall not provide any Key Escrow service.

6.2.4 Private Key Back-Up

(A) The ICA may Back-Up ICA Private Keys insofar as:

(i) each Private Key is protected to a standard which is at least equivalent to that required in relation to the principal Private Key in accordance with this Policy; and

(ii) where more than one Private Key is Backed-Up within a single security environment, each of the Private Keys which is Backed-Up within that environment must be protected to a standard which is at least equivalent to that required in relation to an Issuing ICA Private Key in accordance with this Policy.

6.2.5 Private Key Archival

(A) The ICA shall ensure that no ICA Key which is a Private Key is archived.

6.2.6 Private Key Transfer into or from a Cryptographic Module

(A) The ICA shall ensure that no ICA Private Key is transferred or copied other than:

(i) for the purposes of:

(a) Back-Up;

(b) establishing an appropriate degree of resilience in relation to the provision of the SMKI Services; or

(c) in circumstances where the SMKI PMA has (following consultation with the Security Sub-Committee) given explicit approval to do so in order to maintain continuity of the provision of SMKI Services; and

(ii) in accordance with a level of protection which is compliant with FIPS 140-2 Level 3 (or any equivalent to that Federal Information Processing Standard which updates or replaces it from time to time).

6.2.7 Private Key Storage on Cryptographic Module

See Part 6.2.1 of this Policy.

6.2.8 Method of Activating Private Key

(A) The ICA shall ensure that the Cryptographic Module in which any ICA Private Key is stored may be accessed only by an authorised member of ICA Personnel who has been Authenticated following an Authentication process which:

(i) has an appropriate level of strength to ensure the protection of the Private Key; and

(ii) involves the use of Activation Data.

6.2.9 Method of Deactivating Private Key

(A) The ICA shall ensure that any ICA Private Key shall be capable of being de-activated by means of the ICA Systems, at least by:

(i) the actions of:

(a) turning off the power;

(b) logging off;

(c) carrying out a system reset; and

(ii) a period of inactivity of a length which shall be set out in the IKI CPS.

6.2.10 Method of Destroying Private Key

(A) The ICA shall ensure that the IKI CPS incorporates provisions for the exercise of strict controls in relation to the destruction of ICA Keys.

(B) The ICA shall ensure that no ICA Key (whether in active use, existing as a copy for the purposes of resilience, or Backed-Up) is destroyed except in accordance with a positive decision by the ICA to destroy it.

6.2.11 Cryptographic Module Rating

See Part 6.2.1 of this Policy.

6.3 OTHER ASPECTS OF KEY PAIR MANAGEMENT

6.3.1 Public Key Archival

(A) The ICA shall ensure that it archives ICA Public Keys in accordance with the requirements of Part 5.5 of this Policy.

6.3.2 Certificate Operational Periods and Key Pair Usage Periods

(A) The ICA shall ensure that the Validity Period of each Certificate Issued by it shall be as follows:

(i) in the case of an IKI Certificate, 10 years;

(ii) in the case of an Issuing ICA Certificate, 25 years; and

(iii) in the case of a Root ICA Certificate, 50 years.

(B) For the purposes of paragraph (A), the ICA shall set the ‘notAfter’ value specified in Annex B in accordance with that paragraph.

(C) The ICA shall ensure that no ICA Private Key is used after the end of the Validity Period of the Certificate containing the Public Key which is associated with that Private Key.

6.4 ACTIVATION DATA

6.4.1 Activation Data Generation and Installation

(A) The ICA shall ensure that any Cryptographic Module within which an ICA Key is held has Activation Data that are unique and unpredictable.

(B) The ICA shall ensure that:

(i) these Activation Data, in conjunction with any other access control, shall be of an appropriate level of strength for the purposes of protecting the ICA Keys; and

(ii) where the Activation Data comprise any PINs, passwords or pass-phrases, the ICA shall have the ability to change these at any time.

6.4.2 Activation Data Protection

(A) The ICA shall ensure that the IKI CPS incorporates provision for the use of such cryptographic protections and access controls as are appropriate to protect against the unauthorised use of Activation Data.

6.4.3 Other Aspects of Activation Data

[Not applicable in this Policy]

6.5 COMPUTER SECURITY CONTROLS

6.5.1 Specific Computer Security Technical Requirements

(A) The ICA shall ensure that the IKI CPS incorporates provisions in relation to the identification and implementation, following the conclusion of any threat assessment, of security measures which make provision for at least the following:

(i) the establishment of access controls in relation to the activities of the ICA;

(ii) the appropriate allocation of responsibilities to Privileged Persons;

(iii) the identification and Authentication of organisations, individuals and Systems involved in ICA activities;

(iv) the use of cryptography for communication and the protection of Data stored on the ICA Systems;

(v) the audit of security related events; and

(vi) the use of recovery mechanisms for ICA Keys.

6.5.2 Computer Security Rating

(A) The ICA shall ensure that the IKI CPS incorporates provisions relating to the appropriate security rating of the ICA Systems.

6.6 LIFE-CYCLE TECHNICAL CONTROLS

6.6.1 System Development Controls

(A) The ICA shall ensure that any software which is developed for the purpose of establishing a functionality of the ICA Systems shall:

(i) take place in a controlled environment that is sufficient to protect against the insertion into the software of malicious code;

(ii) be undertaken by a developer which has a quality system that is:

(a) compliant with recognised international standards (such as ISO 9001:2000 or an equivalent standard); or

(b) available for inspection and approval by the SMKI PMA, and has been so inspected and approved.

6.6.2 Security Management Controls

(A) The ICA shall ensure that the IKI CPS incorporates provisions which are designed to ensure that the ICA Systems satisfy the requirements of Section G2 (System Security: Obligations on the DCC) and Section G5 (Information Security: Obligations on the DCC and Users) of the Code.

6.6.3 Life-Cycle Security Controls

See Part 6.6.2 of this Policy.

6.7 NETWORK SECURITY CONTROLS

6.7.1 Use of Offline Root ICA

(A) The ICA shall ensure that its functions as the Root ICA are carried out on a part of the ICA Systems that is neither directly nor indirectly connected to any System which is not a part of the ICA Systems.

6.7.2 Protection Against Attack

(A) The ICA shall use its best endeavours to ensure that the ICA Systems are not Compromised, and in particular for this purpose that they are designed and operated so as to detect and prevent:

(i) any Denial of Service Event; and

(ii) any unauthorised attempt to connect to them.

(B) The ICA shall use its reasonable steps to ensure that the ICA Systems cause or permit to be open at any time only those network ports, and allow only those protocols, which are required at that time for the effective operation of those Systems, and block all network ports and protocols which are not so required.

6.7.3 Separation of Issuing ICA

(A) The DCC shall ensure that, where its functions as the Issuing ICA are carried out on a part of the ICA Systems that is connected to an external network, they are carried out on a System that is Separated from all other ICA Systems.

6.7.4 Health Check of ICA Systems

(A) The ICA shall ensure that, in relation to the ICA Systems, a vulnerability assessment in accordance with Sections G2.13 – G2.15 of the Code (Management of Vulnerabilities) is carried out with such frequency as may be specified from time to time by the Independent SMKI Assurance Service Provider.

6.8 TIME-STAMPING

6.8.1 Use of Time-Stamping

(A) The ICA shall ensure that Time-Stamping takes place in relation to all Certificates and all other ICA activities which require an accurate record of time.

(B) The ICA shall ensure that the ICA incorporates provisions in relation to the time source and mechanisms used by any Time-Stamping Authority which carries out Time-Stamping on behalf of the ICA.

7 CERTIFICATE CRL AND OCSP CONTROLS

7.1 CERTIFICATE PROFILES

The ICA shall use only the Certificate Profiles in Annex B.

7.1.1 Version Number(s)

[Not applicable in this Policy]

7.1.2 Certificate Extensions

[Not applicable in this Policy]

7.1.3 Algorithm Object Identifiers

[Not applicable in this Policy]

7.1.4 Name Forms

[Not applicable in this Policy]

7.1.5 Name Constraints

[Not applicable in this Policy]

7.1.6 Certificate Policy Object Identifier

[Not applicable in this Policy]

7.1.7 Usage of Policy Constraints Extension

[Not applicable in this Policy]

7.1.8 Policy Qualifiers Syntax and Semantics

[Not applicable in this Policy]

7.1.9 Processing Semantics for the Critical Certificate Policies Extension

[Not applicable in this Policy]

7.2 CRL PROFILE

7.2.1 Version Number(s)

(A) The ICA shall ensure that the IKI ARL and IKI CRL conform with X.509 v2 and IETF RFC 5280.

7.2.2 CRL and CRL Entry Extensions

(A) The ICA shall notify Parties of the profile of the IKI CRL and of any IKI CRL extensions.

7.3 OCSP PROFILE

7.3.1 Version Number(s)

[Not applicable in this Policy]

7.3.2 OCSP Extensions

[Not applicable in this Policy]

8 COMPLIANCE AUDIT AND OTHER ASSESSMENTS

8.1 FREQUENCY OR CIRCUMSTANCES OF ASSESSMENT

Provision in relation to this is made in Appendix C of the Code (SMKI Compliance Policy).

8.2 IDENTITY/QUALIFICATIONS OF ASSESSOR

Provision in relation to this is made in Appendix C of the Code (SMKI Compliance Policy).

8.3 ASSESSOR’S RELATIONSHIP TO ASSESSED ENTITY

Provision in relation to this is made in Appendix C of the Code (SMKI Compliance Policy).

8.4 TOPICS COVERED BY ASSESSMENT

Provision in relation to this is made in Appendix C of the Code (SMKI Compliance Policy).

8.5 ACTIONS TAKEN AS A RESULT OF DEFICIENCY

Provision in relation to this is made in Appendix C of the Code (SMKI Compliance Policy).

8.6 COMMUNICATION OF RESULTS

Provision in relation to this is made in Appendix C of the Code (SMKI Compliance Policy).

9 OTHER BUSINESS AND LEGAL MATTERS

In so far as provision is made in relation to all the matters referred to in this Part, it is found in the DCC Licence and the provisions of the Code (including in Section L11 (Subscriber Obligations) and Section L12 (Relying Party Obligations) of the Code).

9.1 FEES

See the statement at the beginning of this Part.

9.1.1 Certificate Issuance or Renewal Fees

See the statement at the beginning of this Part.

9.1.2 IKI Certificate Access Fees

See the statement at the beginning of this Part.

9.1.3 Revocation or Status Information Access Fees

See the statement at the beginning of this Part.

9.1.4 Fees for Other Services

See the statement at the beginning of this Part.

9.1.5 Refund Policy

See the statement at the beginning of this Part.

9.2 FINANCIAL RESPONSIBILITY

9.2.1 Insurance Coverage

See the statement at the beginning of this Part.

9.2.2 Other Assets

See the statement at the beginning of this Part.

9.2.3 Insurance or Warranty Coverage for Subscribers and Subjects

See the statement at the beginning of this Part.

9.3 CONFIDENTIALITY OF BUSINESS INFORMATION

9.3.1 Scope of Confidential Information

See the statement at the beginning of this Part.

9.3.2 Information not within the Scope of Confidential Information

See the statement at the beginning of this Part.

9.3.3 Responsibility to Protect Confidential Information

See the statement at the beginning of this Part.

9.4 PRIVACY OF PERSONAL INFORMATION

9.4.1 Privacy Plan

See the statement at the beginning of this Part.

9.4.2 Information Treated as Private

See the statement at the beginning of this Part.

9.4.3 Information not Deemed Private

See the statement at the beginning of this Part.

9.4.4 Responsibility to Protect Private Information

See the statement at the beginning of this Part.

9.4.5 Notice and Consent to Use Private Information

See the statement at the beginning of this Part.

9.4.6 Disclosure Pursuant to Judicial or Administrative Process

See the statement at the beginning of this Part.

9.4.7 Other Information Disclosure Circumstances

See the statement at the beginning of this Part.

9.5 INTELLECTUAL PROPERTY RIGHTS

See the statement at the beginning of this Part.

9.6 REPRESENTATIONS AND WARRANTIES

9.6.1 Certification Authority Representations and Warranties

See the statement at the beginning of this Part.

9.6.2 Registration Authority Representations and Warranties

See the statement at the beginning of this Part.

9.6.3 Subscriber Representations and Warranties

See the statement at the beginning of this Part.

9.6.4 Relying Party Representations and Warranties

See the statement at the beginning of this Part.

9.6.5 Representations and Warranties of Other Participants

See the statement at the beginning of this Part.

9.7 DISCLAIMERS OF WARRANTIES

See the statement at the beginning of this Part.

9.8 LIMITATIONS OF LIABILITY

See the statement at the beginning of this Part.

9.9 INDEMNITIES

See the statement at the beginning of this Part.

9.10 TERM AND TERMINATION

9.10.1 Term

See the statement at the beginning of this Part.

9.10.2 Termination of IKI Certificate Policy

See the statement at the beginning of this Part.

9.10.3 Effect of Termination and Survival

See the statement at the beginning of this Part.

9.11 INDIVIDUAL NOTICES AND COMMUNICATIONS WITH PARTICIPANTS

9.11.1 Subscribers

See the statement at the beginning of this Part.

9.11.2 IKI Certification Authority

See the statement at the beginning of this Part.

9.11.3 Notification

See the statement at the beginning of this Part.

9.12 AMENDMENTS

9.12.1 Procedure for Amendment

See the statement at the beginning of this Part.

9.12.2 Notification Mechanism and Period

See the statement at the beginning of this Part.

9.12.3 Circumstances under which OID Must be Changed

See the statement at the beginning of this Part.

9.13 DISPUTE RESOLUTION PROVISIONS

See the statement at the beginning of this Part.

9.14 GOVERNING LAW

See the statement at the beginning of this Part.

9.15 COMPLIANCE WITH APPLICABLE LAW

See the statement at the beginning of this Part.

9.16 MISCELLANEOUS PROVISIONS

9.16.1 Entire Agreement

See the statement at the beginning of this Part.

9.16.2 Assignment

See the statement at the beginning of this Part.

9.16.3 Severability

See the statement at the beginning of this Part.

9.16.4 Enforcement (Attorney’s Fees and Waiver of Rights)

See the statement at the beginning of this Part.

9.16.5 Force Majeure

See the statement at the beginning of this Part.

9.17 OTHER PROVISIONS

9.17.1 IKI Certificate Policy Content

See the statement at the beginning of this Part.

9.17.2 Third Party Rights

See the statement at the beginning of this Part.

Annex A: Definitions and Interpretation

In this Policy, except where the context otherwise requires -

- expressions defined in Section A of the Code (Definitions and Interpretation) have the same meaning as is set out in that Section,
- the expressions in the left hand column below shall have the meanings given to them in the right hand column below,
- where any expression is defined in Section A of the Code (Definitions and Interpretation) and in this Annex, the definition in this Annex shall take precedence for the purposes of the Policy.

Activation Data means any private Data (such as a password or the Data on a smartcard) which are used to access a Cryptographic Module.

Archive means the archive of Data created in accordance with Part 5.5.1 of this Policy (and "**Archives**" and "**Archived**" shall be interpreted accordingly).

Audit Log means the audit log created in accordance with Part 5.4.1 of this Policy.

Authentication means the process of establishing that an individual, Certificate, System or Organisation is what he or it claims to be (and "**Authenticate**" shall be interpreted accordingly).

Authorised Responsible Officer (ARO) means an individual that has successfully completed the process for becoming an ARO on behalf of a Party, Manufacturer, an RDP, a DCC Service Provider or SECCo in accordance with the SMKI RAPP.

Authorised Subscriber means a Party, Manufacturer, RDP or SECCo which has successfully completed the procedures set out in this Policy and has been authorised by the ICA to submit a Certificate Signing Request.

Certificate means either an IKI Certificate or an ICA Certificate.

Certificate Profile means a table bearing that title in Annex B and specifying certain parameters to be contained within a Certificate.

Certificate Re-Key means a change to the Public Key contained within a Certificate bearing a particular serial number.

Certificate Revocation Request means a request for the revocation of a Certificate by the ICA, submitted by the Subscriber for that Certificate to the ICA in accordance with the SMKI RAPP and this Policy.

Certificate Signing Request means a request for a Certificate submitted by an Eligible Subscriber in accordance with the SMKI RAPP.

Cryptographic Credential Token has the meaning set out in the SMKI RAPP

Eligible Subscriber Means an Authorised Subscriber and:

a) in respect of each IKI Certificate Issued by the IKI Administrator CA or the IKI Registration Authority CA, the DCC;
b) in respect of each IKI Certificate Issued by the IKI Authorised Organisation Subscriber CA, each Eligible Subscriber in respect of Organisation Certificates;
c) in respect of each IKI Certificate Issued by the IKI Authorised Device Subscriber CA, each Eligible Subscriber in respect of Device Certificates;
d) in respect of each IKI Certificate Issued by the IKI Authorised Web Service Subscriber CA, each Eligible Subscriber for Device Certificates that is the DCC or a Supplier; or
e) in respect of each ICA Certificate, the DCC;
f) in respect of each IKI Certificate Issued by the IKI File Signing Certification Authority, an Authorised Subscriber that is a Party, Manufacturer, RDP or SECCo.

File Signing Certificate means a Certificate Issued by the IKI File Signing Certification Authority.

ICA See IKI Certification Authority

ICA Certificate means either a Root ICA Certificate or an Issuing ICA Certificate.

ICA Key means any Private Key or a Public Key generated by the ICA for the purposes of complying with its obligations under the Code.

ICA Private Key means either a Root ICA Private Key or an Issuing ICA Private Key.

ICA Systems means the Systems used by the ICA in relation to the SMKI Services.

IKI Certification Authority (or ICA) means the DCC, acting in the capacity and exercising the functions of one or more of:

(a) the Root ICA;

(b) the Issuing ICA; and

(c) the Registration Authority.

IKI Administrator Certification Authority (or CA) means the Issuing ICA when performing the function of Issuing IKI Certificates to Registration Authority Personnel, Registration Authority Managers and Authorised Responsible Officers acting on behalf of DCC Service Providers for the purposes of Authenticating such persons to SMKI Services.

IKI Authorised Device Subscriber Certification Authority (or CA) means the Issuing ICA when performing the function of issuing an ICA Certificate for the purposes of authenticating Authorised Responsible Officers to SMKI Services for the purposes of submitting CSRs in respect of Device Certificates over a DCC Gateway Connection.

IKI Authorised Organisation Subscriber Certification Authority (or CA) means the Issuing ICA when performing the function of Issuing Certificates for the purposes of authenticating Authorised Responsible Officers to SMKI Services for the purposes of submitting Certificate Signing Requests (CSRs) and Certificate Revocation Requests (CRRs) in respect of Organisation Certificates over a DCC Gateway Connection.

IKI Authorised Internet Organisation Subscriber Certification Authority (or CA) means the Issuing ICA when performing the function of Issuing Certificates for the purposes of authenticating Authorised Responsible Officers to SMKI Services for the purposes of submitting CSRs and CRRs in respect of Organisation Certificates over the Internet.

IKI Authorised Web Service Subscriber Certification Authority (or CA) means the Issuing ICA when performing the function of Issuing Certificates to Authorised Subscribers for the purposes of authenticating a Subscriber's Systems to SMKI Services for the purposes of submission of CSRs in respect of Device Certificates via the web service interfaces.

IKI Authority Revocation List (or IKI ARL) means a list, produced by the ICA, of all ICA Certificates that have been revoked in accordance with this Policy.

IKI Certificate means a certificate in the form set out in the IKI Certificate Profile in accordance with Annex B and Issued by the Issuing ICA in accordance with this Policy.

IKI Certificate Revocation List (IKI CRL) Means a certificate revocation list issued by the Issuing ICA.

IKI File Signing Certification Authority (or CA) means the Issuing ICA when performing the function of Issuing Certificates to Authorised Responsible Officers for the purpose of signing files related to Threshold Anomaly Detection, SMKI Recovery Procedure and the Certified Products List sent to the DCC.

IKI Registration Authority Certification Authority (or CA) means the Issuing ICA when performing the function of Issuing Certificates to DCC in relation to DCC Systems for the purposes of authenticating such Systems to SMKI Services

Issue means the act of the ICA, in its capacity as the Root ICA or Issuing ICA, and acting in accordance with this Policy, of creating and signing a Certificate which is bound to both a Subject and a Subscriber (and "Issued" and "Issuing" shall be interpreted accordingly).

Issuing ICA Certificate means a certificate in the form set out in the Issuing ICA Certificate Profile in accordance with Annex B and Issued by the Root ICA to the Issuing ICAs in accordance with this Policy. The Issuing ICA may act in one of the following capacities:

a) IKI Administrator CA;

b) IKI Registration Authority CA;

c) IKI Authorised Organisation Subscriber CA;

d) IKI Authorised Device Subscriber CA;

e) IKI Authorised Internet Organisation Subscriber CA;

f) IKI Authorised Web Service Subscriber CA; and

g) IKI File Signing CA

Issuing ICA Private Key means a Private Key which is stored and managed by the ICA acting in its capacity as the Issuing ICA.

Issuing ICA Public Key means the Public Key which is part of a Key Pair with an Issuing ICA Private Key.

Issuing IKI Certification Authority (or Issuing ICA) means the DCC exercising the function of Issuing IKI Certificates to Eligible Subscribers and of storing and managing the Private Keys associated with that function.

Key Escrow means the storage of a Private Key by a person other than the Subscriber or Subject of the Certificate which contains the related Public Key.

Object Identifier (or OID) means an Object Identifier assigned by the Internet Address Naming Authority.

Private Key Material in relation to a Private Key, means that Private Key and the input parameters necessary to establish, use and maintain it.

Registration Authority (RA) means the DCC exercising the function of receiving and processing Certificate Signing Requests made in accordance with the SMKI RAPP.

Registration Authority Manager means either a director of the DCC or any other person who may be identified as such in accordance with the SMKI RAPP.

Registration Authority Personnel means those persons who are engaged by the DCC, in so far as such persons carry out, or are authorised to carry out, any function of the Registration Authority.

Relying Party means a person who, pursuant to the Code, receives and relies upon a Certificate.

Root ICA Private Key means a Private Key which is stored and managed by the ICA acting in its capacity as the Root ICA.

Root ICA Certificate means a certificate in the form set out in the Root ICA Certificate Profile in accordance with Annex B and self-signed by the Root ICA in accordance with this Policy.

Root IKI Certification Authority (or Root ICA) means the DCC exercising the function of Issuing ICA Certificates to the Issuing ICA and storing and managing Private Keys associated with that function.

Security Related Functionality means the functionality of the ICA Systems which is designed to detect, prevent or mitigate the adverse effect of any Compromise of that System.

Subject means:

- in relation to an IKI Certificate, the entity or object identified by the Distinguished Name in the ‘Subject field of the IKI Certificate Profile. The Distinguished Name of the subject of an IKI Certificate is as set out in Annex B; and
- in relation to an ICA Certificate, the globally unique name of the Root ICA or Issuing ICA as identified in the ‘Subject’ field of the relevant Certificate Profile in Annex B.

Subscriber means, in relation to any Certificate, a Party, Manufacturer, RDP or SECCo which has been Issued with and accepted that Certificate, acting in its capacity as the holder of the Certificate.

Time-Stamping means the act that takes place when a Time-Stamping Authority, in relation to a Certificate, stamps a particular datum with an accurate indicator of the time (in hours, minutes and seconds) at which the activity of stamping takes place.

Time-Stamping Authority means that part of the ICA that:

(a) where required, provides an appropriately precise time-stamp in the format required by this Policy; and

(b) relies on a time source that is:

(i) accurate;

(ii) determined in a manner that is independent of any other part of the ICA Systems; and

(iii) such that the time of any time-stamp can be verified to be that of the Independent Time Source at the time at which the time-stamp was applied.

Validity Period means, in respect of a Certificate, the period of time for which that Certificate is intended to be valid.

Annex B: ICA Certificate and IKI Certificate Profiles

Certificate Structure and Contents

This Annex lays out requirements as to structure and content with which ICA Certificates and IKI Certificates shall comply. All terms in this Annex shall, where not defined in the Code, this Policy, or the GB Companion Specification, have the meanings in IETF RFC 5280.

Common requirements applicable to Root ICA Certificates, Issuing ICA Certificates and IKI Certificates

All ICA Certificates and IKI Certificates that are validly authorised within the SMKI for use within the scope of GB Smart Metering:

- shall be compliant with IETF RFC 5280;
- contain the `authorityKeyIdentifier` extension, except where the Certificate is the Root ICA Certificate;
- contain the `keyUsage` extension which shall be marked as critical;
- be X.509 v3 certificates as defined in IETF RFC 5280, encoded using the ASN.1 Distinguished Encoding Rules;
- only contain Public Keys that are 4096-bit RSA Public Keys for the Root ICA Certificate or 2048-bit RSA Public Keys for all subordinate certificates which shall include Issuing OCA Certificates;
- only provide for signature methods that are RSA with SHA 256
- contain a `certificatePolicies` extension containing at least one PolicyIdentifier which shall be marked as critical. For clarity and in adherence with IETF RFC 5280, Certification Path Validation undertaken by Parties shall interpret this extension;
- contain a `serialNumber` of no more than 16 octets in length;
- contain a `subjectKeyIdentifier` which shall be marked as non-critical;
- contain an `authorityKeyIdentifier` in the form *option [0]* `KeyIdentifier` which shall be marked as non-critical, except where the Certificate is the Root ICA Certificate. Note this exception only applies where RemotePartyRole as specified in the `X520OrganizationalUnitName` field = root;
- only contain `keyIdentifiers` generated as per method (2) of Section 4.2.1.2 of IETF RFC 5280;

- contain an issuer name which MUST be identical to the signer's subject name; and
- have a valid notBefore field set to the time of issue and a valid notAfter field expiration date as per IETF RFC 5280 Section 4.1.2.5.

Requirements applicable to IKI Certificates only

All IKI Certificates that are Issued by an Issuing ICA shall:

- contain a non-empty subject field which for:
  - IKI Certificates issued by the IKI Administrator CA, shall contain an X520organisationalName attribute whose value shall be set to that of the Authorised Subscriber, an X520OrganizationalUnitName attribute whose value shall be set to ADMIN, a X520commonName attribute whose value shall be set to the individual’s name and an X520emailAddress attribute whose value shall be set to the individual’s email address;
  - IKI Certificates issued by the IKI Registration Authority CA, shall contain an organisationalName whose value shall be set to that of the Authorised Subscriber, an X520OrganizationalUnitName attribute whose value shall be set to one of ‘RA’, ‘MULTI_ALLOWED’ or ‘Super RA’ and a X520commonName attribute whose value shall be set to the individual’s name;
  - IKI Certificates issued by the IKI Authorised Organisation Subscriber CA, shall contain an X520OrganizationalName attribute whose value shall be set to that of the Authorised Subscriber, an X520OrganizationalUnitName attribute whose value shall be set to the two octet hexadecimal representation of the RemotePartyRole that this Certificate allows the subject of the certificate to request SMKI Organisation Certificates under and a X520 commonName attribute whose value shall be set to the ARO’s name;
  - IKI Certificates issued by the IKI Authorised Device Subscriber CA, shall contain an X520OrganizationalName attribute whose value shall be set to that of the Authorised Subscriber, an X520OrganizationalUnitName attribute whose value shall be set to the two octet hexadecimal representation of the RemotePartyRole that this Certificate allows the subject of the certificate to request SMKI Organisation Certificates under and a X520commonName attribute whose value shall be set to the ARO’s or system name
  - IKI Certificates issued by the IKI Authorised Web Service Subscriber CA, shall contain an X520OrganizationalName attribute whose value shall be set to that of

    the Authorised Subscriber, an X520OrganizationalUnitName attribute whose value shall be set to the two octet hexadecimal representation of the RemotePartyRole that this Certificate allows the subject of the certificate to request SMKI Organisation Certificates under and a X520commonName attribute whose value shall be set to the system's name.

  - IKI Certificates issued by the IKI Authorised Internet Organisation Subscriber CA, shall contain an X520OrganizationalName attribute whose value shall be set to that of the Authorised Subscriber, an X520OrganizationalUnitName attribute whose value shall be set to the two octet hexadecimal representation of the RemotePartyRole that this Certificate allows the subject of the certificate to request SMKI Organisation Certificates underand a X520commonName attribute whose value shall be set to the ARO's name;
  - IKI Certificates issued by the IKI File Signing CA, shall contain an X520organisationalName attribute whose value shall be set to that of the Authorised Subscriber, an X520OrganizationalUnitName attribute whose value shall be set to two octet hexadecimal representation of the RemotePartyRole that this Certificate allows the subject of the certificate to request SMKI Organisation Certificates under, a second X520OrganizationalUnitName attribute whose value should be set to the Party Signifier of the Authorised Subscriber and a X520commonName attribute whose value shall be set to the ARO's name.
- contain a single Public Key;
- contain a `keyUsage` extension marked as critical, with a value of:
  - `digitalSignature`;
- For Certificates Issued by the IKI Administrator CA, IKI Authorised Organisation Subscriber CA, IKI Authorised Internet Device Subscriber CA, IKI Authorised Internet Organisation Subscriber CA, IKI Authorised Wed Service Subscriber CA and IKI Registration Authority CA, contain a extKeyUsage extension marked critical, with a value of:
  - `clientAuth`.
- contain a single policyIdentifier in the `certificatePolicies` extension that refers to the OID of this Policy under which the Certificate is Issued.

Requirements applicable ICA Certificates only

All ICA Certificates Issued by the Root ICA shall:

- be such that, per RFC5280, the `IssuerName` is identical to the signer's SubjectName;

- have a subject name field unique within the Root ICA;
- contain a single public key;
- contain a keyUsage extension marked as critical and defined as:
    - keyCertSign; and
    - cRLSign;
- for Issuing ICA Certificates, contain at least one policyIdentifier in the certificatePolicies extension that refers to the OID of this Policy under which the Certificate is Issued;
- for the Root ICA Certificate, contain a single policyIdentifier in the certificatePolicies extension that refers to the OID for any Policy;
- for Issuing ICA Certificates, contain the basicConstraints extension, with values cA=True, and pathLen=0. This extension shall be marked as critical;
- for the Root ICA Certificate, contain the basicConstraints extension, with the value cA=True and pathLen absent (unlimited). This extension shall be marked as critical.

IKI Certificate Profile

Field Name	RFC 5759/5280 Type	Value	Reference
Version	Integer	V3	
serialNumber	Integer	Positive Integer of up to 16 Octets	
signature	AlgorithmIdentifier	SHA256 With RSA encryption	
issuer	Name	Globally unique name of Issuing ICA	
Authoritykeyidentifier	KeyIdentifier	A unique value that matches the subjectKeyIdentifier of the issuer's credential	

subjectKeyIdentifier	KeyIdentifier	Provides a means for identifying certificates containing the particular Public Key used in an application	
notBefore	Time	Creation time of the Certificate	
notAfter	Time	Expiry time of the Certificate	
subject	Name	Name of the Subject of the Certificate	
subjectPublicKeyInfo	SubjectPublicKeyInfo	The subject's Public Key	
extensions	Extensions	Critical and non-critical extensions	
signatureAlgorithm	AlgorithmIdentifier	2048 bit RSA and SHA256	
signatureValue	BIT STRING	Subject IKI Certificate signature	

Interpretation

`version`

The version of the X.509 IKI Certificate. Valid IKI Certificates shall identify themselves as version 3.

`serialNumber`

IKI Certificate serial number, a positive integer of up to 16 octets. The `serialNumber` identifies the IKI Certificate, and shall be created by the Issuing ICA that signs the IKI Certificate. The `serialNumber` shall be unique in the scope of IKI Certificate signed by the Issuing ICA.

`signature`

The identity of the signature algorithm used to sign the IKI Certificate. The field is identical to the value of the IKI Certificate 'signatureAlgorithm' field explained further under the next '**signatureAlgorithm**' heading below.

`issuer`

The name of the signer of the IKI Certificate. This will be the gloablly unique name of the Issuing ICA.

`authorityKeyIdentifier`

To optimize building the correct credential chain, the non-critical Authority Key Identifier extension shall be populated with a unique value as recommended by RFC 5280 and shall be included in all IKI Certificates. The IKI Certificate shall contain an `authorityKeyIdentifier` in the form *option [0]* `KeyIdentifier`.

`subjectKeyIdentifier`

The Subject Key Identifier extension shall be included and marked as non-critical in the IKI Certificate. The IKI Certificate shall contain a `subjectKeyIdentifier` with KeyIdentifier generated as per method (2) of Section 4.2.1.2 of IETF RFC 5280 and which shall always be 8 octets in length.

`validity`

The time period over which the Issuing ICA expects the IKI Certificate to be valid. The validity period is the period of time from `notBefore` through `notAfter`, inclusive.

All times shall be stated in the Universal Coordinated Time (UTC) time zone. Times up to and including 23:59:59 December 31, 2049 UTC shall be encoded as UTCTime as YYMMDDHHmmssZ.

Times later than 23:59:59 December 31, 2049 UTC shall be encoded as GeneralizedTime as YYYYMMDDHHmmssZ.

`notBefore`

The earliest time an IKI Certificate may be used. This shall be the time the IKI Certificate is created.

`notAfter`

The latest time an IKI Certificate is expected to be used. The value in a `notAfter` field shall be treated as specified in RFC 5280.

`subject`

The formatting of this field shall contain a unique X.500 Distinguished Name (DN) with the value as defined earlier in the Requirements Sections in Annex B to this IKI Certificate Policy.

`subjectPublicKeyInfo`

The IKI Certificate `subjectPublicKeyInfo` field shall indicate the Public Key algorithm identifier and the Public Key in the specified algorithm format as specified in RFC 5280.The object identifiers for the supported algorithms and the methods for encoding the Public Key materials (public key and parameters) are specified in RFC3279, RFC4055, and RFC4491.

The algorithm field shall use the following identifier:

```
rsaEncryption ::= {iso(1) member-body(2) us(840)
rsadsi(113549) pkcs(1) pkcs-1(1) rsaEncryption(1)}
```

The `rsaEncryption` OID is intended to be used in the algorithm field of a value of type AlgorithmIdentifier. The parameters field MUST have `ASN`.1 type NULL for this algorithm identifier.

The RSA public key MUST be encoded using the ASN.1 type RSAPublicKey:

```
RSAPublicKey ::= SEQUENCE {

          modulus              INTEGER,     -- n

          publicExponent       INTEGER  }   -- e
```

where `modulus` is the modulus n, and publicExponent is the public exponent e. The DER encoded `RSAPublicKey` is the value of the BIT STRING `subjectPublicKey`.

signatureAlgorithm

The `signatureAlgorithm` field shall indicate the Issuing ICA signature algorithm used to sign this IKI Certificate is as defined under the next '**Signature Method**' heading below.

signatureValue

The Issuing ICA's signature of the IKI Certificate is computed using the Issuing ICA's private RSA 2048-bit IKI Certificate signing key using the algorithm identified under the next '**Signature Method (RSA)**' heading below.

The IKI Certificates shall be signed by the Issuing ICA using the RSA algorithm identified under the next '**Signature Method (RSA)**' heading below. The structure for RSA signatures is as per RFC 5280.

extensions

IKI Certificates SHOULD contain the extensions described below. They SHOULD NOT contain any additional extensions:

- `certificatePolicy`: critical; OID as a policyIdentifier
- `keyUsage`: critical; digitalSignature.
- `extKeyUsage`: critical;clientAuth[1]

[1] The `extKeyUsage` extension is not used in IKI Certificates Issued by the IKI File Signing CA.

- `basicConstraints`: critical; cA=false.
- `authorityKeyIdentifier`.
- `subjectKeyIdentifier`.
- `cRLDistributionPoint`: non-critical; URI string, which shall identify the URL of the IKI CRL
- Private extensions used internally by the SMKI application with an extension OID of 2.16.840.1.113733.1.16.3, 2.16.840.1.113733.1.16.4, 2.16.840.1.113733.1.16.5 or 2.16.840.1.113733.1.16.11 where:
  - 2.16.840.1.113733.1.16.3 - Contains Cert Profile OID
  - 2.16.840.1.113733.1.16.4 - Contains Account ID
  - 2.16.840.1.113733.1.16.5 - Contains Base64 encoded URL for Symantec PKI Client web service.
  - 2.16.840.1.113733.1.6.11 - Containd Jurisdiction Hash of Symantec Master account

Cryptographic Primitives for Signature Method

Signature Method (RSA)

The RSA signature method is defined in NIST FIPS 186-4. When implementing RSA, the SHA-256 message digest algorithm choice is identified based on section 5 of SP 800-57part1.

The signature algorithm shall be `SHA256-with-RSA` Encryption as specified in RFC4055. The algorithm identifier is:

```
sha256WithRSAEncryption(11) ::= {iso(1) member-body(2)
us(840) rsadsi(113549) pkcs(1) pkcs-1(1)
sha256WithRSAEncryption(11)}
```

SHA-256 hash algorithm

The hash algorithm used by the IKI Certificate shall be the SHA-256 secure hash algorithm as defined in NIST FIPS 180-4.

Root ICA Certificate Profile

Field Name	RFC 5759/5280 Type	Value	Reference
`version`	`Integer`	V3	
`serialNumber`	`Integer`	Positive Integer of up to 16 Octets	

signature	AlgorithmIdentifier	SHA256 With RSA Encryption	
issuer	Name	Globally unique name of Root ICA	
subjectKeyIdentifier	KeyIdentifier	A unique value that matches the subjectKeyIdentifier of the issuer's credential	
notBefore	Time	Creation time of the Certificate	
notAfter	Time	Expiry time of the Certificate	
subject	Name	Unique name of Root ICA (same as issuer name)	
subjectPublicKeyInfo	SubjectPublicKeyInfo	The subject's Public Key	
extensions	Extensions	Critical and non-critical extensions	
signatureAlgorithm	AlgorithmIdentifier	4096 bit RSA and SHA256	
signatureValue	BIT STRING	Subject Certificate signature	

These certificates are the root of trust for the IKI

version

The version of the X.509 Certificate. Valid Certificates shall identify themselves as version 3.

serialNumber

Certificate serial number, a positive integer of up to 16 octets. The serialNumber identifies the Certificate, and shall be created by the ICA Certificate that signs the Certificate (self-signed by Root ICA). The `serialNumber` shall be unique in the scope of Certificates signed by the ICA Certificate.

`signature`

The identity of the signature algorithm used to sign the Certificate. The field is identical to the value of the Root CA Certificate's `signatureAlgorithm` field explained further under the next '**Signature Method'** heading below.

`issuer`

The name of the signer of the Certificate. This will be the gloablly unique name of the Root ICA. This will be the same as the `subject` as it is self-signed by the Root ICA.

`subjectKeyIdentifier`

The Root ICA credentials contain the `subjectKeyIdentifier` extension. Adding `subjectKeyIdentifer` facilitates certificate path building, which is necessary to validate credentials.

The Subject Key Identifier extension shall be included and marked as non-critical in the Certificate. The Certificate shall contain a `subjectKeyIdentifier` with `KeyIdentifier` generated as per method (2) of Section 4.2.1.2 of IETF RFC 5280.

`validity`

The time period over which the issuer expects the Certificate to be valid for. The validity period is the period of time from `notBefore` through `notAfter`, inclusive.

All times shall be stated in the Universal Coordinated Time (UTC) time zone. Times up to and including 23:59:59 December 31, 2049 UTC shall be encoded as UTCTime as YYMMDDHHmmssZ.

Times later than 23:59:59 December 31, 2049 UTC shall be encoded as `GeneralizedTime` as YYYYMMDDHHmmssZ.

`notBefore`

The earliest time a Certificate may be used. This shall be the time the Certificate is created.

notAfter

The latest time a Certificate is expected to be used. The value in a `notAfter` field shall be treated as specified in RFC 5280.

subject

This field must be populated with the globally unique name of the Root ICA.

subjectPublicKeyInfo

The Root ICA Certificate `subjectPublicKeyInfo` field shall indicate the Public Key algorithm identifier and the Public Key in the specified algorithm format as specified in RFC 5280, where the key size shall be 4096-bit RSA. The object identifiers for the supported algorithms and the methods for encoding the public key materials (public key and parameters) are specified in RFC3279, RFC4055, and RFC4491.

The algorithm field shall use the following identifier:

```
rsaEncryption ::= {iso(1) member-body(2) us(840)
rsadsi(113549) pkcs(1) pkcs-1(1) rsaEncryption(1)}
```

The `rsaEncryption` OID is intended to be used in the algorithm field of a value of type `algorithmIdentifier`. The parameters field MUST have ASN.1 type NULL for this algorithm identifier.

The RSA public key MUST be encoded using the ASN.1 type RSAPublicKey:

```
RSAPublicKey ::= SEQUENCE {

    modulus             INTEGER,    -- n

    publicExponent      INTEGER  }  -- e
```

where modulus is the modulus n, and `publicExponent` is the public exponent e. The DER encoded `RSAPublicKey` is the value of the BIT STRING `subjectPublicKey`.

signatureAlgorithm

The `signatureAlgorithm` field shall indicate the Root ICA signature algorithm used to sign this Certificate as defined in section under the next '**Signature Method**' heading below.

`signatureValue`

The Root ICA's signature of the Certificate is computed using the Root ICA's private RSA 4096-bit Certificate signing key using the algorithm identified under the next '**Signature Method (RSA)**' heading below.

The Root ICA Certificates shall be signed by the Root ICA using the RSA algorithm identified under the next '**Signature Method (RSA)**' heading below. The structure for RSA signatures is as per RFC 5280.

`extensions`

Certificates MUST contain the extensions described below and MUST have the name form as described. They SHOULD NOT contain any additional extensions:

`extensions`

- o `certificatePolicy`: critical; OID as a policyIdentifier
- o `keyUsage`: critical; keyCertSign, crlSign
- o `basicConstraints`: critical; cA=true, pathLen absent (unlimited)
- o `subjectKeyIdentifer`: non-critical; Method 2

Cryptographic Primitives for Signature Method

Signature Method (RSA)

The RSA signature method is defined in NIST FIPS 186-4. When implementing RSA, the SHA-256 message digest algorithm choice is identified based on section 5 of SP 800-57part1.

The signature algorithm shall be `SHA256-with-RSA` Encryption as specified in RFC4055. The algorithm identifier is:

```
sha256WithRSAEncryption(11) ::= {iso(1) member-body(2)
us(840) rsadsi(113549) pkcs(1) pkcs-1(1)
sha256WithRSAEncryption(11)}
```

SHA-256 hash algorithm

The hash algorithm used by the Certificate shall be the SHA-256 secure hash algorithm as defined in NIST FIPS 180-4.

Issuing ICA Certificate Profile

Field Name	**RFC 5759/5280 Type**	**Value**	**Reference**
version	Integer	V3	
serialNumber	Integer	Positive Integer of up to 16 Octets	
signature	AlgorithmIdentifier	SHA256 With RSA Encryption.	
issuer	Name	Unique name of Root ICA	
subjectKeyIdentifier	KeyIdentifier	A unique value that matches the subjectKeyIdentifier of the issuer's credential	
authorityKeyIdentifier	KeyIdentifier	A unique value that matches the subjectKeyIdentifier of the issuer's credential	
notBefore	Time	Creation time of the certificate	
notAfter	Time	Expiry time of the Certificate	
subject	Name	Unique name of Issuing ICA within the Root ICA	

subjectPublicKeyInfo	SubjectPublicKeyInfo	The subject's Public Key	
extensions	Extensions	Critical and non-critical extensions	
signatureAlgorithm	AlgorithmIdentifier	2048-bit RSA and SHA256	
signatureValue	BIT STRING	Subject certificate signature	

version

The version of the X.509 Certificate. Valid Certificates shall identify themselves as version 3.

serialNumber

Certificate serial number, a positive integer of up to 16 octets. The serialNumber identifies the Certificate, and shall be created by the Root ICA that signs the Certificate. The serialNumber shall be unique in the scope of Certificates signed by the Root ICA.

signature

The identity of the signature algorithm used to sign the Certificate. The field is identical to the value of the Issuing ICA Certificate's signatureAlgorithm field explained further under the next '**signatureAlgorithm**' heading below.

issuer

The name of the signer of the Certificate. This will be the gloablly unique name of the Root ICA.

subjectKeyIdentifier

The Issued credentials contain the subjectKeyIdentifier extension. Adding subjectKeyIdentifer facilitates certificate path building, which is necessary to validate credentials.

The Subject Key Identifier extension shall be included and marked as non-critical in the Certificate. The Certificate shall contain a subjectKeyIdentifier with KeyIdentifier generated as per method (2) of Section 4.2.1.2 of IETF RFC 5280 and which shall always be 8 octets in length.

`authorityKeyIdentifier`

To optimize building the correct credential chain, the non-critical Authority Key Identifier extension shall be populated with a unique value as recommended by RFC 5280 and shall be included in all IKI Certificates. The Certificates shall contain a `authorityKeyIdentifier` in the form *option [0]* `KeyIdentifier`.

`validity`

The time period over which the issuer expects the Certificate to be valid for. The validity period is the period of time from `notBefore` through `notAfter`, inclusive.

All times shall be stated in the Universal Coordinated Time (UTC) time zone. Times up to and including 23:59:59 December 31, 2049 UTC shall be encoded as `UTCTime` as YYMMDDHHmmssZ.

Times later than 23:59:59 December 31, 2049 UTC shall be encoded as `GeneralizedTime` as YYYYMMDDHHmmssZ.

`notBefore`

The earliest time a Certificate may be used. This shall be the time the Certificate is created.

`notAfter`

The latest time a Certificate is expected to be used. The value in a `notAfter` field shall be treated as specified in RFC 5280.

`subject`

This field must be populated with the globally unique name of the Issuing ICA.

`subjectPublicKeyInfo` (RSA)

The Issuing ICA Certificate `subjectPublicKeyInfo` field shall indicate the Public Key algorithm identifier and the Public Key in the specified algorithm format as specified in RFC 5280, where the key size shall be 2048-bit RSA. The object identifiers for the supported algorithms and the methods for encoding the public key materials (public key and parameters) are specified in RFC3279, RFC4055, and RFC4491.

The algorithm field shall use the following identifier:

```
rsaEncryption ::= {iso(1) member-body(2) us(840)
rsadsi(113549) pkcs(1) pkcs-1(1) rsaEncryption(1)}
```

The `rsaEncryption` OID is intended to be used in the algorithm field of a value of type `AlgorithmIdentifier`. The parameters field MUST have `ASN`.1 type `NULL` for this algorithm identifier.

The RSA public key MUST be encoded using the `ASN`.1 type `RSAPublicKey`:

```
      RSAPublicKey ::= SEQUENCE {

         modulus            INTEGER,    -- n

         publicExponent     INTEGER  }  -- e
```

where `modulus` is the modulus n, and `publicExponent` is the public exponent e. The DER encoded `RSAPublicKey` is the value of the BIT STRING `subjectPublicKey`.

`signatureAlgorithm`

The `signatureAlgorithm` field shall indicate the Root ICA signature algorithm used to sign this Certificate as defined under the next '**Signature Method**' heading below.

`signatureValue`

The Root ICA's signature of the Certificate is computed using the Root ICA's private RSA 4096-bit private signing key using the algorithm identified under the next '**Signature Method (RSA)**' heading below.

The Certificates shall be signed by the Root ICA using the `RSA` algorithm identified under the next '**Signature Method (RSA)**' heading below. The structure for RSA signatures is as per RFC 5280.

`extensions`

Issuing ICA certificates MUST contain the extensions described below and MUST have the name form as described. They SHOULD NOT contain any additional extensions:

- o `certificatePolicy`: critical; OID as a policyIdentifier
- o `keyUsage`: critical; keyCertSign, crlSign

- `basicConstraints`: critical; cA=true, pathLen=0
- `subjectKeyIdentifer`: non-critical; Method 2
- `authorityKeyIdentifier`: non-critical; Option [0]
- `subjectAltName`: non-critical; pointer in the form of an X500 directory name for the associated Private Key on the relevant Cryptographic Module in which the Private Key is stored.
- `cRLDistributionPoint`: non-critical; URI string

Cryptographic Primitives for Signature Method

Signature Method (RSA)

The RSA signature method is defined in NIST FIPS 186-4. When implementing RSA, the SHA-256 message digest algorithm choice is identified based on section 5 of SP 800-57 part1.

The signature algorithm shall be `SHA256-with-RSA` Encryption as specified in RFC4055. The algorithm identifier is:

```
sha256WithRSAEncryption(11) ::= {iso(1) member-body(2)
us(840) rsadsi(113549) pkcs(1) pkcs-1(1)
sha256WithRSAEncryption(11)}
```

SHA-256 hash algorithm

The hash algorithm used by the Certificate shall be the SHA-256 secure hash algorithm as defined in NIST FIPS 180-4.

Version R5.0

Appendix R

Common Test Scenarios Document

Contents

1. Introduction

1.1. Purpose

1.1.1 The purpose of this document is to:

a) Define the procedural steps to be undertaken by a Party wishing to complete User Entry Process Tests (UEPT) in accordance with SEC Section H14;

b) Set out the User Entry Process Tests that must be conducted by the Relevant Party with regard to each User Role that it may want to fulfil; and

c) Describe the role and responsibilities with regard to the conduct of UEPT, including;

- Entry and exit requirements
- Defining Test Scripts
- Defining Test Data

- Planning the manner in which tests will be undertaken
- Executing the tests
- Reporting the results of those tests to the Data Communications Company (DCC) for approval.

1.1.2 Additionally, this document sets out the above for a Testing Participant wishing to complete Testing in respect of additional Service Requests post completion of UEPT ("Additional SR Testing").

1.2. Types of Testing Required

1.2.1 Clause 8 Annex C sets out:

a) the specific tests that are required to be performed for a new Party seeking to undertake User Entry Process Testing;

b) A complete list of Service Requests that shall be required to be tested prior to being sent to DCC Live Systems.

1.3. Not Used

1.4. Additional SR Testing

1.4.1 Where a Party has completed UEPT for a User Role and is looking to become:

a) An Eligible User for Service Requests that were previously excluded from that Party's scope for UEPT; and/or

b) An Eligible User for any Service Requests that have been introduced since the Party completed UEPT for a User Role in which they operate,

and is seeking to complete Additional SR Testing, then all clauses of this CTSD shall apply to the undertaking of Additional SR Testing, except for Clause 5.3 (Self Service Interface testing) and Clause 8.1.27 which shall not apply.

2. Scope

2.1.1. Section 8 Annex C: Test Scenarios of this document sets out:

a) The User Entry Process Tests as required by SEC Section H14; and

b) A complete list of Service Requests that shall be required to be tested prior to being sent to DCC Live Systems.

3. Test Sequence

3.1.1. The Relevant Party may undertake the test scenarios that are set out in this document in any sequence. The testing of the constituent Service Requests that comprise the SMETS2+ Install and Commission test scenario shall be undertaken in a sequence that is set out in Section C clause 8.1.2.

4. Test Certificates & Security Requirements

4.1.1. For the purposes of gaining IKI, SMKI and DCCKI Test Certificates Testing Participants should refer to the Enduring Testing Approach Document.

4.1.2. Each Testing Participant must comply with the Security Requirements set out in the Enduring Testing Approach Document.

5. UEPT and Additional SR Testing Procedure

This section describes the procedure that must be completed in order for Parties to complete UEPT or Additional SR Testing.

5.1. SMETS2+ Install and Commission

5.1.1 The SMETS2+ Install and Commission test scenario tests the Relevant Party's ability to send Service Requests to support the installation and commissioning of SMETS2+ Devices, and to receive the consequential communications and alerts. Service Requests are set out in a specific order within the test scenarios for this purpose and the Relevant Party must execute Test Scripts in the order set out in the test scenario in Section C clause 8.1.2.

5.2. DUIS Service Requests

5.2.1 Clause 8.1.4 sets out the Service Requests that a Party is required to have tested prior to it being eligible to send those Service Requests in a particular User Role. The full list of Service Requests is set out in Clause 8.1.4 (8.1.4 DUIS Matrix) together with the type of testing that they apply to.

Descoping of DUIS Service Requests

5.2.2 Excluding the Self-Service Interface test set out in Clause 5.3, a Test Participant may request to descope Service Request(s) (including descoping of a Command Variant), Device Alert(s), DCC Alert(s) or a Response Code(s) from UEPT as set out in Clause 8.1.4 where:

a) the Testing Participant will not use this functionality in the DCC Live Systems and therefore does not wish to become an Eligible User for the relevant Service Requests; or

b) the Testing Participant is unable to produce a Response Code due to their internal system's error handling.

5.2.3 Descoping a Service Request would mean that a Testing Participant would not become eligible to send that Service Request in a particular User Role in DCC Live Systems

5.2.4 Each request by a Testing Participant to descope a Service Request, Device Alert, DCC Alert or a Response Code is subject to DCC's agreement or, where referred pursuant to Clause 5.2.7, a Panel determination

5.2.5 Anything that a Testing Participant wishes to descope, must be submitted to DCC via their notification of intent to undertake UEPT and via their UEPT Test Plan. As part of this submission the Testing Participant must set out their rationale for the descoping.

5.2.6 DCC will review any submission pursuant to Clause 5.2.5 and shall confirm to the Testing Participant in writing if DCC agrees with this descoping or not in line with the timelines set out in Table 1of this document. In the case of UEPT, where the DCC reasonably considers that the proposed descoping set out by the Testing Participant does not fulfil the minimum set of Service Requests that would be required for that Testing Participant to operate in its User Role, the DCC will not agree to the proposed descoping.

5.2.7 Where the DCC and the Testing Participant do not agree on any individual or group of tests proposed for descoping, as requested by the Testing Participant, the Testing Participant may refer the matter to the Panel for its determination whose decision on which tests may be descoped shall be final and binding.

5.2.8 Where:

a) the Testing Participant is in agreement with the DCC on the tests that may be de-scoped, then the Testing Participant must undertake any tests that DCC does not agree to descope in addition to those that were not proposed for de-scoping; or

b) the Testing Participant has referred the matter to the Panel for determination pursuant to Clade 5.2.7, the Testing Participant must undertake any tests that the Panel has decided should not be de-scoped in addition to those that were not proposed for de-scoping

5.2.9 Should a referral be made to the Panel pursuant to Clause 5.2.7, then the Testing Participant may continue with the UEPT procedural steps for those tests that are not being disputed.

5.2.10 Where a Testing Participant subsequently wishes to be eligible to send a Service Request in the DCC Live Systems for which it has not yet undertaken either UEPT or Additional SR Testing then it must, prior to sending that Service Request in DCC Live Systems, successfully test this either via the UEPT procedural steps (as documented in Table 1, Table 3 and Table 5) or the Additional SR Testing procedural steps (as documented in Table 2, Table 4 and Table 6).

5.3. Self-Service Interface (SSI)

5.3.1 For the purpose of UEPT a Relevant Party must produce and execute Test Scripts that demonstrate that the Relevant Party can access the SSI system to the extent permitted by its User Role and to the extent set out in the SSI Interface Specification as defined in SEC Section H8.15.

5.4. Additional SR Testing

5.4.1 A Testing Participant who has completed UEPT for a User Role and is seeking to become:

a) An Eligible User for Service Requests that were previously descoped from their prior completion of UEPT; or

b) An Eligible User for any Service Requests that have been introduced since the Party completed UEPT for a User Role in which they operate,

will not be an Eligible User for any descoped or newly introduced Service Requests in a particular User Role until they have completed testing of the descoped or newly introduced Service Requests in respect of that User Role.

5.4.2 Additional SR Testing may be completed by the following routes:

a) Via the process as documented in Table 1, Table 3 and Table 5.

b) Via Device and User System Testing (DUST) as documented in Table 2, Table 4 and Table 6, where the Testing Participant is already actively participating in DUST.

If a Testing Participant that has previously completed UEPT in a particular User Role is not currently active in DUST, but wishes to use the process in Tables 2, 4 and 6 for Additional SR Testing in respect of that User Role, they must complete the entry process into the test environment used for DUST, as set out in Table 1 of the Enduring Test Approach Document, prior to being able to carry out such testing. The Testing Participant must receive confirmation from DCC of successful completion of Additional SR Testing of the Service Request(s) being tested prior to carrying out further testing of such Service Request(s) in DUST.

5.5. User Entry Process Tests Initiation

5.5.1 The Relevant Party and the DCC shall each use reasonable steps to comply with the timescales that are defined within the procedures in Table 1, Table 4 & Table 7.

5.5.2 In the event that the Relevant Party or the DCC does not comply with the timescales in Table 1, Table 4 & Table 7, the DCC will reschedule subsequent activities to occur as soon as reasonably practicable and the DCC may reschedule that Party's test execution date.

5.6. Procedural Steps for Initiation of User Entry Process Tests

5.6.1 The table below sets out the steps that must be undertaken during Initiation of the UEPT by both the DCC and the Relevant Party seeking to undertake UEPT and the timeframes within which such steps must be complete.

Ref	When	Action	From	To	Information Required	Method
5.6.1.1	60 Working Days (WD) prior to commencement of User Entry Process Tests	Notify DCC of intention to undertake User Entry Process Tests	Relevant Party	DCC	Party notification of intention to undertake testing, including • Name of Party • Confirmation that notification provided to the Code Administrator, User Role(s) • Test start date • Identity of test manager and contact details • if applicable, Services Requests, Device Alerts, DCC Alerts and Response Codes to be descoped	By email as attachment
5.6.1.2	Within 2 WD of receipt of the notification 5.6.1.1	Acknowledge request	DCC	Relevant Party	Confirmation of Party notification including: • Name of Party • User Roles and test start date • DCC User Entry Process Tests test manager contact • Date for User Entry Process Tests initiation meeting	By email as attachment
5.6.1.3	Within 5 WD of receipt of the notification 5.6.1.2	Conduct User Entry Process Tests Initiation Meeting	DCC	Relevant Party	DCC to provide guidance information on conducting User Entry Process Tests, including clarification of test artefacts requirements and access to test environments and if applicable feedback	Meeting

					on descoping of Service Requests, Device Alerts, DCC Alerts and Response Codes.	
5.6.1.4	In each week occurring within the period from 40 WD prior to start of testing	Provide progress report, demonstrating readiness to begin tests	Relevant Party	DCC	Test Readiness Report	By email as attachment
5.6.1.5	25 WD prior to start of testing	Provide test artefacts to support conduct of User Entry Process Tests	Relevant Party	DCC	Test Plan incorporating the Test Schedule and, if applicable, Services Requests, Device Alerts, DCC Alerts and Response Codes to be descoped Requirements Traceability Matrix (see clause 6. 7) Test Scripts (see clause 6.8) Test Data Plan (see clause 7)	By email as attachments
5.6.1.6	By 20 WD prior to start of testing	DCC complete review of test artefacts	DCC	Relevant Party	Details regarding any deficiencies in the test artefacts provided including feedback on descoping of Service Requests, Device Alerts, DCC Alerts and Response Codes, if applicable, and a revised start date for testing, where necessary – continue from 5. 6.1.7. Or confirmation that test artefacts accepted including agreement to descope Service Requests, if applicable – continue from 5. 6.1.9.	By email as attachments
5.6.1.7	By 10 WD prior to start of testing	Relevant Party to provide revised documents	Relevant Party	DCC	Revised documents	By email as attachments
5.6.1.8	By 7 WD prior to start of testing	DCC complete review of revised test artefacts	DCC	Relevant Party	Details regarding any deficiencies in the test artefacts and a revised start date for testing provided where necessary – Regress and continue from 5. 6.1.7. Or confirmation that test artefacts accepted –continue from 5. 6.1.9.	By email as attachments
5.6.1.9	By 5 WD prior to start of testing	Review Test Readiness Report and confirm the Entry Criteria for commencing testing in relation to the relevant User Role has been met Confirm Start Date and Test Schedule for execution of tests by Relevant Party	DCC Quality Gate meeting	Relevant Party	**Source:** Test Readiness Report, Test Schedule **Output:** Confirmation of Relevant party readiness to proceed	Quality Gate review meeting Published via secure communications
	If there is any outstanding documentation presented at the Quality Gate Review the DCC shall assess it as part of its assessment of the entry criteria under clause 5.8.					

Table 1 UEPT Initiation: Procedural Steps

5.7. Procedural Steps for Initiation of Additional SR Testing via DUST

5.7.1 The table below sets out the steps that must be undertaken during initiation of the Additional SR Testing by both the DCC and the Testing Participant seeking to undertake such testing via DUST and the timeframes within which such steps must be complete.

5.7.2 For Testing Participants wishing to carry out Additional SR Testing via the UEPT process, DCC and Testing Participant should follow the steps and timeframes as set out in Table 1 in Clause 5.6.1.

Ref	When	Action	From	To	Information Required	Method
5.7.2.1	At least 15 Working Days (WD) prior to commencement of Additional SR Tests	Notify DCC of intention to undertake Additional SR Tests	Relevant Party	DCC	Party notification of intention to undertake testing, including Name of Party User Role(s) The Service Reference Variant(s) of the additional Service Requests(s) to be tested Test start date Identity of test manager and contact details	By email as attachment
5.72.2	Within 2 WD of receipt of the notification 5.7.2.1	Acknowledge request	DCC	Relevant Party	Confirmation of Party notification including: Name of Party User Roles and test start date The Service Reference Variant(s) of the additional Service Requests(s) to be tested Provide any applicable User Guidance	By email as attachment

Table 2 Additional SR Testing Initiation: Procedural Steps

5.8. UEPT Entry Criteria

5.8.1 Each Party wishing to undertake UEPT must comply with (and, where specified below, provide evidence of complying with) the following criteria prior to entry into UEPT:

a) Prior to start of test execution, the DCC must confirm with the Code Administrator that the person requesting to commence testing has acceded to the SEC;

b) The Relevant Party must have identified the User Roles for which it wishes to undertake UEPT;

c) All relevant test artefacts (as agreed with the DCC and set out in clause 5.6, 5.9, and 5.17) must have been produced by the Relevant Party and approved by the DCC. This includes:

- Party Notification of Intention to Undertake Testing
- Test Readiness Report
- Test Plan incorporating the Test Schedule
- Requirements Traceability Matrix
- Test Scripts

- Test Data Plan;

d) The Relevant Party has provided evidence to the DCC that a test environment capable of supporting the planned testing has been established and is available;

e) The Relevant Party has provided evidence to the DCC that an appropriate level of resources are available to support the UEPT process; and

f) The Relevant Party has provided confirmation that the Security Requirements set out in the Enduring Testing Approach Document have been met.

5.8.2 Pursuant to H14.15 where the DCC considers that the Relevant Party has not met the Entry Criteria for the User Role for which it is seeking to undertake testing, the DCC may:

a) Prevent the Relevant Party from undertaking UEPT for a particular User Role until such time as the DCC is satisfied that the Relevant Party meets the Entry Criteria; and

b) Reschedule the test start date for the Relevant Party for that particular User Role. In so doing, the DCC shall provide the earliest practicable alternative date; or

c) Provide provisional approval of the Test Readiness Report (and approval to proceed) with an understanding that the outstanding documentation would be provided before the start of testing otherwise testing will not commence.

5.8.3 Where the DCC is not satisfied that a Relevant Party meets the Entry Criteria to commence testing, the Relevant Party may refer the matter to the Panel, pursuant to SEC Section H14.16. Where the Panel determines that the Relevant Party has met the entry criteria the DCC shall schedule the start of testing as soon as reasonably practical.

5.9. User Entry Process Tests Execution

5.10. Procedural Steps for User Entry Process Tests Execution

5.10.1 The table below sets out the steps that must be undertaken during test execution by either the DCC or Relevant Party seeking to undertake User Entry Process Tests and the timeframes within which such steps must be complete as set out in the Test Schedule which will be updated by the Relevant Party from time to time to reflect test progress.

Ref	When	Action	From	To	Information Required	Method
5.10.1.1	User Entry Process Tests Start Date	Confirm connectivity (of Relevant Party's test environment) to DCC test environment where this has not already happened as a result of earlier testing.	Relevant Party	DCC	Test Results achieved	As directed by DCC
5.10.1.2	In accordance with Test Schedule and completion of 5.6.5.1	Conduct User Entry Process Tests	Relevant Party		Approved test artefacts.	As per test artefacts
5.10.1.3	Daily Basis, or alternative schedule agreed with DCC	Provide progress report to DCC	Relevant Party	DCC	Test Execution Dashboard, including details of testing issues identified	By email as attachment
5.10.1.4	User Entry Process Tests execution complete	Provide Test Completion report	Relevant Party	DCC	User Entry Process Tests completion report including details of Test Scripts executed and testing issues	By email as attachment

					resolved and Test Evidence for all tests completed	

Table 3 UEPT Execution: Procedural Steps

5.10.2 Note: Confirming connectivity is to verify that the Testing Participant's system can connect to the DCC test environment and that the Testing Participant's system is capable of successfully sending Service Requests to and receiving Acknowledgements from the DCC System. The DUIS Connectivity Test consists of up to three test scenarios: one for each test webservice available to the Testing Participant*. This comprises:

a) Sending a DCC-only Service Request and receiving an Acknowledgement/Response;

b) Sending a Critical pre-command and receiving the Transformed message; and

c) Sending a Non-Critical Service Request and receiving an Acknowledgement.

d) This test does not need to be repeated as a subsequent part of UEPT.

5.10.3 Note: If the Testing Participant would not have access to a particular webservice once it has qualified in the User Role for which it is undertaking UEPT the test will not be required.

5.11. Procedural Steps for the Execution of Additional SR Testing via DUST

5.11.1 The table below sets out the steps that must be undertaken during execution of the Additional SR Testing by both the DCC and the Testing Participant seeking to undertake Additional SR Testing via DUST and the timeframes within which such steps must be complete.

5.11.2 For Testing Participant wishing to carry Additional SR Testing via the UEPT process, DCC and Testing Participant should follow the steps and timeframes as set out in Table 3 in Clause 5.10.1.

Ref	When	Action	From	To	Information Required	Method
5.11.2.1	User Entry Process Tests Start Date	Confirm Test execution has started	Relevant Party	DCC		Email
5.11.2.2	In accordance with the Testing Participant's test schedule	Conduct Additional SR Testing	Relevant Party			
5.11.2.3	Daily Basis, or alternative schedule agreed with DCC	Provide progress report to DCC	Relevant Party	DCC	Test Execution Dashboard, including details of testing issues identified	By email as attachment
5.11.2.4	Additional SR Testing execution complete	Provide completed Test Execution Dashboard and Test Evidence	Relevant Party	DCC	Test Execution Dashboard, including details of testing issues identified and Test Evidence for all test completed	By email as attachment

Table 4 Additional SR Testing Execution: Procedural Steps

5.12. Test Suspension/Resumption in UEPT and Additional SR Testing

5.12.1 During the execution of tests, the DCC or the Relevant Party each have the right to suspend testing where it considers that this is reasonably necessary.

5.12.2 Testing will only recommence when agreed by both the DCC and the Relevant Party.

5.13. Possible Suspension Criteria

5.13.1 Reasonable grounds for suspending testing may include any of the following:

a) Application components are not available as scheduled;

b) A Testing Issue prevents further useful testing from proceeding;

c) A significant percentage of planned Test Scripts for a given day fail, taking Testing Issue severity and volume of tests into consideration which would generate root cause analysis to be undertaken to establish the cause. Testing Issues trending should also be used to determine any recommendation. The outcome of any root cause analysis activity may result in testing being suspended;

d) Test Scripts to be executed are in a “blocked” status due to an identified Testing Issue; or

e) The Relevant Party has failed to comply with the procedural steps in Table 3 for executing UEPT or Table 4 for executing Additional SR Testing.

5.14. Test Resumption Criteria

5.14.1 Where testing has been suspended, either the DCC or the Relevant Party as appropriate shall produce a test suspension report reflecting the cause of the suspension, and what actions are to be taken by whom and when in order for testing to resume – the Test Resumption Criteria. The DCC and the Relevant Party shall take reasonable steps to support each other to achieve the Test Resumption Criteria.

5.14.2 Testing will only resume once the DCC or Relevant Party has demonstrated to the other Party’s satisfaction that the Test Resumption Criteria have been met.

5.15. Disputes regarding Test Suspension/Resumption

5.15.1 Any dispute regarding the suspension or resumption of UEPT shall be heard in accordance with Section H14.18A of the SEC. Any dispute regarding the suspension or resumption of Additional SR Testing shall follow the same procedure as that set out in H14.18A Where a dispute regarding the suspension/resumption of testing is made, testing will not resume whilst the dispute is being heard, or until the Test Resumption Criteria are met by the DCC or the Relevant Party

5.16. User Entry Process Tests Completion

5.17. Procedural Steps for User Entry Process Tests Completion

5.17.1 The table below sets out the steps that must be undertaken during test completion by either the DCC or Relevant Party and the timeframes within which such steps must be complete.

Ref	When	Action	From	To	Information Required	Method

5.17.1.1	Within 2 WD of receipt of the report in 5.10.1.4	Confirm receipt of notification of Test complete (Test Completion Report)	DCC	Relevant Party	User Entry Process Tests Test Completion Report	By email
5.17.1.2	Within 5 WD of receipt of the notification 5.17.1.1	DCC review completion report and confirm that User Entry Process Tests concluded, or further testing required	DCC	Relevant Party	User Entry Process Tests completion report and supporting artefacts as requested by DCC set out in 5.10.1.1 refers	Quality Gate review meeting (see clause 5.20)
5.17.1.3	Within 2 WD of successful quality gate review meeting	Confirm Test Complete	DCC	Relevant Party	Issue Test Completion Certificate (see clause 10)	By email as attachment

Table 5 UEPT Completion: Procedural Steps

5.17.2 Notwithstanding 5.17.1.2 above pursuant to H14.19 the DCC shall confirm on request by the Relevant Party whether or not it considers that the Relevant Party has successfully completed UEPT.

5.18. Procedural Steps for Additional SR Testing Completion

5.18.1 The table below sets out the steps that must be undertaken during test completion by either the DCC or Relevant Party and the timeframes within which such steps must be complete.

5.18.2 For Testing Participant wishing to carry Additional SR Testing via the UEPT process, DCC and Testing Participant should follow the steps and timeframes as set out in Table 5 in Clause 5.17.1.

Ref	When	Action	From	To	Information Required	Method
5.18.1.1	Within 2 WD of receipt of 5.11.2.4	Confirm receipt of notification of Test complete	DCC	Relevant Party	Completed Test Execution Dashboard and Test Evidence	By email
5.18.1.2	Within 5 WD of receipt of the notification 5.18.1.1	DCC review test evidence and execution dashboard and confirm that Additional SR Testing concluded, or further testing required	DCC	Relevant Party	Completed Test Execution Dashboard and Test Evidence	By email
5.18.1.3	Within 2 WD of successful review of Test Evidence	Confirm Test Complete	DCC	Relevant Party	Issue Authority to Proceed into Production Certificate	By email as attachment

Table 6 Additional SR Testing Completion: Procedural Steps

5.19. UEPT or Additional SR Testing Exit Criteria

5.19.1 The following Exit Criteria are to be met prior to a Relevant Party's completion of and exit from UEPT or from Additional SR Testing, unless stated otherwise:

a) All Tests have been executed and results have been documented by the Relevant Party and evidence captured in the Relevant Party's Test Management Tool and is available to be provided to the DCC;

b) All testing issues identified during a Relevant Party's test execution have been recorded in the Test Management Tool, of those Testing Issues either:

- the Testing Issue generated by the Relevant Party has been fixed and verified by retest; or
- Where outstanding, the Testing Issue has been reviewed and documented, and been included as part of a remediation plan that outlines the next steps to be taken, including estimated timescales required to resolve each of their outstanding Testing Issues. The remediation plan must be agreed by the DCC;

c) any outstanding Testing Issue count must not exceed those defined in Table 7, below:

Severity***	Threshold for Outstanding Testing Issues for UEPT	Threshold for Outstanding Testing Issues for Additional SR Testing
1	0	0
2	0	0
3	5*	3*
4	10*	5*
5	As agreed**	As agreed**

Table 7 Testing Issue Threshold

* - Work around and remediation plan to be agreed with the DCC for each issue that ensures no impact on other Users or the DCC

** - As agreed with the DCC,

*** - Refer to Annex G for definitions of Issue severities.

d) A Test Completion Report has been created by the Relevant Party and approved by the DCC. If the Relevant Party is conducting Additional SR Testing via DUST this exit criterion does not apply.

e) A Quality Gate Review meeting has been held between the Relevant Party, if the Relevant Party is undertaking either UEPT or Additional SR Testing via UEPT, and the DCC, with progress approved by the DCC. If the Relevant Party is conducting Additional SR Testing via DUST this exit criterion does not apply.

5.19.2 Upon completion of the criteria above a Test Completion Certificate will be issued to the Relevant Party by the DCC. Where test completion criteria have not been met the Relevant Party will need to reschedule testing with the DCC subject to the availability of the DCC test environment.

5.19.3 In the case of UEPT, pursuant to SEC Section H14.21, where the DCC considers that a Party has not met the Exit Criteria, that Party may refer the matter to the Panel. In the case of Additional SR Testing, where the DCC is not satisfied that a Party has successfully completed Additional SR Testing (for a particular User Role), that Party may refer the matter to the Panel for its determination. Where the Party disagrees with any such determination of the Panel, then the Party may refer the matter to the Authority for its determination (which shall be final and binding for the purposes of this Code).

5.19.4 Where a dispute regarding whether a Party has met either the UEPT or the Additional SR Testing Exit Criteria occurs, the completion process will not resume whilst the dispute is being heard by the Panel, or until the relevant Exit Criteria are met by the Relevant Party.

5.19.5 Where the Panel decided that the Exit Criteria have been met the DCC shall supply a Test Completion Certificate to the Relevant Party.

5.20. Quality Gate Review

5.20.1 A final decision regarding whether a Party has successfully completed UEPT or Additional SR Testing will be provided to the Relevant Party no later than 2 Working Days after the date on which a quality gate review meeting is held.

5.20.2 In addition, pursuant to H14.19, the DCC shall confirm on request by the Relevant Party whether or not it considers that the Relevant Party has successfully completed UEPT.

5.21. UEPT and Additional SR Test Completion Certificate

5.21.1 The UEPT and Additional SR Test Completion Certificate shall be issued by the DCC to the Relevant Party for a specified User Role once the quality gate review has concluded that the Relevant Party has met the UEPT Exit Criteria for the specified User Role. This Certificate shall identify the Service Requests in respect of which the Relevant Party successfully executed UEPT and for which the Relevant Party is now an Eligible User in the specified User Role.

5.21.2 The UEPT and Additional SR Test Completion Certificate shall be updated and re-issued by the DCC to the Relevant Party once the quality gate review or review of test evidence, as specified in Clause 5.17.1.2, has concluded that the Relevant Party has met the Additional SR Testing Exit Criteria for those Service Requests for the specified User Role. This Certificate shall identify the additional Service Requests that have been successfully executed in Additional SR Testing, in addition to those for which the Relevant Party has previously completed testing, and for which the Relevant Party is an Eligible User in the specified User Role.

6. Annex A: Test Artefacts

The DCC and each Relevant Party will be required to produce and maintain a number of documents, dashboards and reports during the testing lifecycle as depicted in Figure 1 Test Documentation Hierarchy, below.

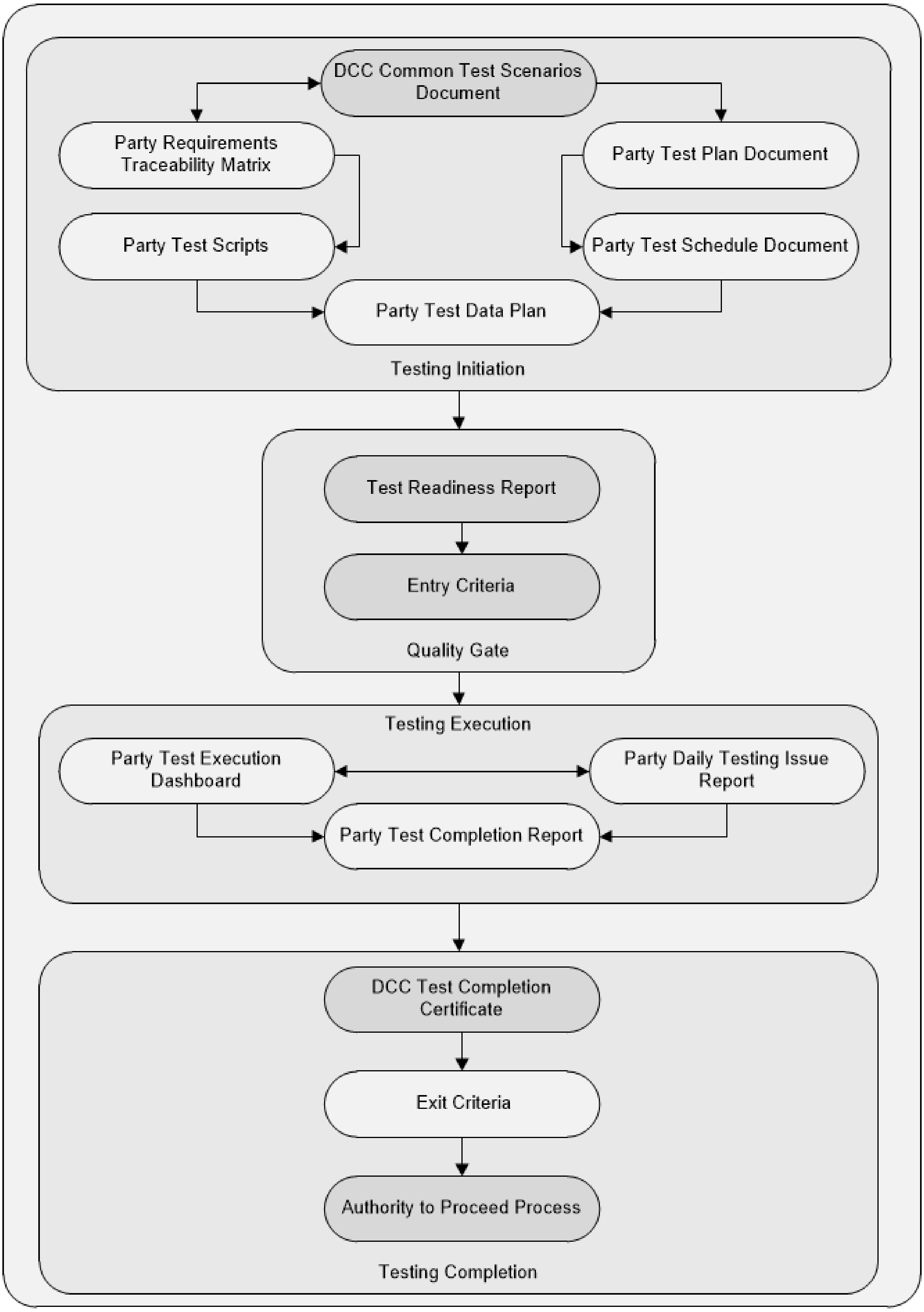

DCC Common Test Scenarios Document
Party Requirements Traceability Matrix
Party Test Plan Document
Party Test Scripts
Party Test Schedule Document
Party Test Data Plan
Testing Initiation
Test Readiness Report
Entry Criteria
Quality Gate
Testing Execution
Party Test Execution Dashboard
Party Daily Testing Issue Report
Party Test Completion Report
DCC Test Completion Certificate
Exit Criteria
Authority to Proceed Process
Testing Completion

Figure 1 Test Documentation Hierarchy

Party Documents & Reports

6.1. Test Preparation Document Set

6.1.1 The following documentation must be produced by a Relevant Party before Testing commences:

a) Test Plan including Test Schedule;

b) Test Data (see clause 7/Annex B);

c) Requirements Traceability Matrix (see clause 6.7); and

d) Test Scripts (see clause 6.8).

6.2. Reports and Dashboard

6.2.1 Table 8 Test Stage Supporting Documentation Set sets out the Reports and Dashboard that a Party must produce to demonstrate progress in preparing for and executing testing.

6.3. Test Readiness Report (TRR)

6.3.1 The Test Readiness Report shall be produced by the Relevant Party if they are conducting either UEPT or Additional SR Testing via UEPT.

6.3.2 A Test Readiness Report template shall be provided by the DCC.

6.3.3 The report must be provided to the DCC by the Relevant Party on a weekly basis, commencing 40 Working Days prior to the start of Testing and must indicate progress against the following criteria:

a) Previous Test Stage Exit Criteria (if appropriate);

b) Relevant Party Test tool selected and available;

c) Relevant Party key RAID (Risk, Assumption, Issue and Dependency) items, including, for each key item that has the potential to cause significant disruption to the commencement and / or completion of User Entry Process Tests or Additional SR Testing via UEPT:

- Priority (High, Medium, Low)
- Severities of open issues
- Action taken
- Target close date
- Overall RAG status (based on progress to plan)

d) Relevant Party Test Plan produced;

e) Relevant Party Test Schedule produced;

f) Relevant Party Requirements Traceability Matrix % complete to date

- Total numbers of requirements identified
- Actual number of testable requirements in progress
- Actual number of testable requirements not started
- Actual number of requirements deemed not testable;

g) Relevant Party Test Script % complete to date – to reflect the following breakdown

- Planned number of Test Scripts
- Actual number of Test Scripts produced to date
- Actual number of Test Scripts in progress
- Actual number of Test Scripts not started;

h) % Test Data readiness by Relevant Party against planned Test Scripts;

i) Readiness of Relevant Party test resources and technical (support) resource;

j) Relevant Party test environment readiness – to include

- User Roles identified;
- Environment configuration approved as suitable – to include;
- Breakdown and description of hardware.

6.4. Test Plan

6.4.1 The Test Plan shall be produced by the Relevant Party if they are conducting either UEPT or Additional SR Testing via UEPT

6.4.2 A Test Plan template shall be provided by the DCC.

6.4.3 The report must be provided to the DCC by the Relevant Party 25 Working Days prior to the start of Testing and will include:

a) Scope of testing, including any Service Requests, Device Alerts, DCC Alerts and/or Response Code the Testing Participant wishes to descope along with rationale for the request to descope;

b) Any items out of scope of testing

c) Features to be tested (referencing relevant sub-clauses within clause 8 of the Common Test Scenarios Document);

d) Approach to testing;

e) Test Schedule to include tests planned for each day; and

f) Resources.

6.5. Test Execution Dashboard

6.5.1 The Test Execution Dashboard will identify the Relevant Party's progress when executing UEPT or Additional SR Testing and will be provided in a reasonable format specified by the DCC. The dashboard must be updated by the Party and provided to the DCC on a daily basis once testing commences, or per an alternative schedule agreed with the DCC.

6.5.2 The dashboard will include the following details:

a) Name of Relevant Party under test;

b) Relevant Party Location of testing;

c) Date and time test execution dashboard updated by Relevant Party;

d) Total number of tests Relevant Party scheduled for execution and projected as a test execution glide path;

e) Actual number of tests executed by Relevant Party (by test run) to date reflected on an incremental daily count including Test Results (passed, failed, blocked, not run, ready for test);

f) Relevant Party summary of Testing Issues to include;

- Total number of Testing Issues generated
- Counts by status Open, Fixed, Closed etc
- Counts by Severity 1, 2, 3 etc

g) Relevant Party Regression Test execution results;

h) Relevant Party summary progress against Exit Criteria;

i) Relevant Party Top 5 risks and issues - to include any environment concerns; and

j) Relevant Party Overall RAG status (based on progress against test schedule).

6.6. Test Completion Report

6.6.1 The Relevant Party, who is conducting either UEPT or Additional SR Testing via UEPT, shall produce a Test Completion Report and submit the draft to the DCC 10 Working Days prior to the test completion date. The finalised version of the Test Completion Report will be submitted to the DCC on completion of each test execution activity.

6.6.2 A Test Completion Report template shall be provided by the DCC to ensure that all Party reports contain the same level of detail. The report will include:

a) Relevant Party Test approach and Scope of Testing Undertaken;

b) Details of updates made to the test environment during the course of testing;

c) Relevant Party Summary of the Test Results

- Total number of tests originally scheduled for execution
- Total number of tests executed (Displayed by test run to include Overall results achieved Passed, Failed, Blocked, Not Run);
- Relevant Party Summary of Testing Issues
- Total number of Testing Issues generated
- Total counts by status Open, Fixed, Closed etc
- Total counts by Severity.

6.6.3 Any tests not run, blocked or not successfully executed must be supported by an explanation.

6.7. Test Traceability

6.7.1 To provide the DCC with a sufficient level of test assurance, all tests executed by each Party undertaking either UEPT or Additional SR Testing via UEPT will be required to demonstrate full traceability as follows:

a) Each requirement captured in the Requirements Traceability Matrix that can be tested must be linked to one or many Test Scripts;

b) Each Test Script executed must be reflected in one or many test execution cycles;

c) A record of each test executed and the results of that test;

d) Where an executed test generates a Testing Issue;

- Each Testing Issue must be linked to the test that generated the Testing Issue
- Any subsequent retesting to validate a fix of Testing Issue carried out must be linked to the Testing Issue
- Each retest executed must reflect a result achieved as a result of execution.

6.8. Test Scripts

6.8.1 A Relevant Party shall develop its own test scripts and demonstrate how those test scripts meet the requirements in accordance with SEC Section H14.17.

	Test Stage Supporting Documentation Set							
No	Phase	Description	DCC Responsibility	Party Responsibility	When/Frequency	Entry Criteria	Exit Criteria	Sign-Off Authority
1	Initiation	Test Plan including Test Schedule	Review and Approve	Produce and maintain	Test Stage Entry Quality Gate and updated during execution as required in preparation for Test Stage Exit Quality Gate	Y	Y	DCC
2	Initiation	Requirements Traceability Matrix	Review and Approve	Produce and maintain	Test Stage Entry Quality Gate and updated during execution as required in	Y	Y	DCC

					preparation for Test Stage Exit Quality Gate			
3	Initiation	Test Scripts	Review and Approve	Produce and maintain	Test Stage Entry Quality Gate and updated during execution as required in preparation for Test Stage Exit Quality Gate	Y	Y	DCC
4	Initiation	Test Data Plan	Review	Produce and maintain	Test Stage Entry Quality Gate and updated during execution as required in preparation for Test Stage Exit Quality Gate	Y	N	DCC
5	Initiation	Test Readiness Review Report	Provide Template Review and Approve	Produce and maintain	Test Stage Entry Quality Gate	Y	N	DCC
6	Initiation	Test Stage Entry Criteria (part of final Test Readiness Report)	Review and Approve	Produce	Test Stage Entry Quality Gate	Y	N	DCC
7	Execution	Test Execution Dashboard	Review	Produce and maintain	Produced and updated daily (or other scheduled agreed with the DCC) during execution in preparation for Test Stage Exit Quality Gate	N	Y	DCC
8	Execution	Test Completion Report	Provide Template Review and Approve	Produce and file	Test Stage during execution in preparation for Test Stage Exit Quality Gate	N	Y	DCC
9	Execution	Test Stage Quality Gate Exit Criteria (part of Test Completion Report)	Review and Approve	Produce	Test Stage Exit Quality Gate	N	Y	DCC

Table 8 Test Stage Supporting Documentation Set

Once these steps are complete the DCC will issue a Test Completion Certificate (see clause 10).

7. Annex B: Test Data

A Test Data Plan will be developed by the Relevant Party and coordinated with DCC in accordance with clause 5.6.1.5. The DCC and Relevant Party will be responsible for set up of Test Data on their respective system which must be defined in the Relevant Party Test Data Plan. The Data defined will be based on the following principles:

No personal data which identifies any individual will be used for testing, but anonymised live Data is acceptable;

Test Data will be representative of data likely to be used in the live environment once the Relevant Party is eligible to send the Service Request in the relevant User Role;

A full range of Test Data covering all services to be tested will be used.

Co-ordination/Segregation of data usage between Relevant Parties testing during the same period will be managed by the DCC.

Table 9 Test Data Responsibilities below outlines the responsibilities in regard to preparing Test Data required to support UEPT.

Deliverable / Activity	Accountable / Responsible	Support
Test Data Preparation	DCC Licensee, Relevant Party	DSP

Table 9 Test Data Responsibilities

8. Annex C: Test Scenarios

8.1.1. Test Scenarios

The following sub clauses contain the test scenarios that reflect the Service Requests applicable to each prospective User Role.

8.1.2. SMETS2+ Install and Commission

ID	IC01*
Title:	Install & Commission the following devices, when the Relevant Party will be supplying Gas: • Communication Hub specified for Region • Gas Meter
Prerequisite:	• Relevant Party holds a Gas Supply Licence • Connection to DCC Test Laboratory • Appropriate data • Available Meter and Communication Hubs • SM WAN Available • Appropriate Security Keys have been installed in the available metering equipment • Required security credentials are present on the Communications Hub

Note: the scope of this test is intentionally limited to only those activities where there is a prescribed order for the submission Service Requests and where failure to follow this order will lead to a failed installation.

Steps	Description	Objective	Actions	Acceptance Criteria
1	Pre-Installation	Notify DCC of Device ID and device details Ascertain the security credentials are installed on the devices	The following Service Requests have been designed to support Pre-Installation: DUIS SR 12.2 – Device Pre-notification * (n) devices	The DCC has received notification of the Device ID Acknowledgement received for relevant Service Request sent
2	White List Device	Identify the Communication Hub to Meter device relationship by: Add the HAN device to HAN device log, by including the MAC addresses and the install codes	Complete the following Service Request to support white listing of device: DUIS SR 8.11- Update HAN Device Log * (n) devices	Service Responses received for all Service Requests sent Service User will receive the following Alert code when the device has been added to the white list: DCC Alert N24

3	Commission	Send response to commission device service request to Service User Update inventory status Configure the Meter: Set Time	Complete the following Service Request to support device commission: DUIS SR 8.1.1 – Commission Device * (n) devices	Acknowledgement received for all Service Requests sent
4	Commission Gas Proxy	To hand over Gas Proxy Function from DSP to the Relevant Party, complete the following: Send Service Request to change credentials to Relevant Party's credentials Ensure Relevant Party can update other credentials as required	Complete the following Service Request to support Commission Gas Proxy Function: DUIS SR 6.21 – Request Handover of DCC Controlled Device * (n) devices	Relevant Party receives an Service Response to confirm the credentials have been changed from the DSP to Relevant Party
5	Join Device	Join Gas meter to GPF	The following Service Requests have been designed to support joining HAN devices: DUIS SR 8.7.2 – Join Service (Non-Critical) **Note:** The following DUIS SRs can be sent during this step, should they not have been sent during steps 1 to 3: DUIS SR 12.2 – Device Pre-notification * (n) devices DUIS SR 8.11- Update HAN Device Log * (n) devices	Relevant Party receives acknowledgement to confirm the HAN devices are joined Acknowledgement received for all Service Requests sent
6	Set MPxN on GSME for display purposes	Set MPxN on GSME for display purposes	Complete the following Service Request to support setting the MPxN on the GSME for display purposes DUIS SR 6.20.1 – Set Device Configuration (Import MPxN)	Relevant party receives a service response to confirm successful execution of the Service Request.

ID	IC02*
Title:	Install & Commission the following devices, when the Relevant Party will be supplying Electricity: Communication Hub specified for Region Electricity Meter
Prerequisite:	Relevant Party holds an Electricity Supply Licence Connection to DCC Test Laboratory Appropriate data Available Meter and Communication Hubs SM WAN Available Appropriate Security Keys have been installed in the available metering equipment Required security credentials are present on the Communications Hub

Note: the scope of this test is intentionally limited to only those activities where there is a prescribed order for the submission Service Requests and where failure to follow this order will lead to a failed installation.

Steps	Description	Objective	Actions	Acceptance Criteria
1	Pre-Installation	Notify DCC of Device ID and device details	The following Service Requests and Self-Service Interface Use Cases have been designed to support Pre-Installation:	The DCC has received notification of the Device ID

		Ascertain the security credentials are installed on the devices	DUIS SR 12.2 – Device Pre-notification * (n) devices	Acknowledgement received for relevant Service Requests sent
2	White List Device	Identify the Communication Hub to Meter device relationship by: Add the HAN device to HAN device log, by including the MAC addresses and the install codes	Complete the following Service Request to support white listing of device: DUIS SR 8.11 - Update HAN Device Log * (n) devices	Service Responses received for all Service Requests sent Service User will receive the following Alert code when the device has been added to the white list: DCC Alert N24
3	Commission	Send response to commission device Service Request to Service User Update Smart Metering Inventory status Configure the Meter: Set Time	Complete the following Service Request to support device commission: DUIS SR 8.1.1 – Commission Device * (n) devices	Acknowledgement received for all Service Requests sent
4	Set MPxN on ESME for display purposes	Set MPxN on ESME for display purposes	Complete the following Service Request to support setting the MPxN on the ESME for display purposes DUIS SR 6.20.1 – Set Device Configuration (Import MPxN)	Relevant party receives a service response to confirm successful execution of the Service Request.

8.1.3. DUIS

The scenarios outlined in this clause are the high-level Test scenarios which are supported by the DUIS Test Matrix in clause 8.1.4. For example, Scenario SR01 refers to all Tests mandated in column CV1 – On Demand in the DUIS Matrix.

ID	SR01
Title:	Non-Critical Command with a command variant of CV1 and a Mode of Operation of On Demand
Scenario	Exercise Non-Critical On Demand Service Requests using Command Variant CV1 applicable to the User Role

ID	SR02
Title:	Non-Critical Command with a command variant of CV1 and a Mode of Operation of Future Dated (either DCC or Device, as determined by DUIS)
Scenario	Exercise Non-Critical Future Dated Service Requests using Command Variant CV1 applicable to the User Role

ID	SR03
Title:	Non-Critical Command with a command variant of CV2 and a Mode of Operation of On Demand
Scenario	Exercise Non-Critical On Demand Service Requests using Command Variant CV2 applicable to the User Role

ID	SR04
Title:	Non-Critical Command with a command variant of CV3 and a Mode of Operation of On Demand
Scenario	Exercise Non-Critical On Demand Service Requests using Command Variant CV3 applicable to the User Role

ID	SR05
Title:	Critical Command with a command variant of CV4 and a Mode of Operation of On Demand
Scenario	Exercise Critical On Demand Service Requests using Command Variant CV4 applicable to the User Role

ID	SR06
Title:	Critical Command with a command variant of CV5 and a Mode of Operation of On Demand
Scenario	Exercise Critical On Demand Service Requests using Command Variant CV5 applicable to the User Role

ID	SR07
Title:	Critical Command with a command variant of CV5 and a Mode of Operation of Future Dated (either DCC or Device, as determined by DUIS)
Scenario	Exercise Critical Future Dated Service Request using Command Variant CV5 applicable to the User Role

ID	SR08
Title:	Critical Command with a command variant of CV6 and a Mode of Operation of On Demand
Scenario	Exercise Critical On Demand Service Request using Command Variant CV6 applicable to the User Role

ID	SR09
Title:	Critical Command with a command variant of CV7 and a Mode of Operation of On Demand
Scenario	Exercise Critical On Demand Service Request using Command Variant CV7 applicable to the User Role

ID	SR010
Title:	Service Requests with a command variant of CV8
Scenario	Exercise Service Request using Command Variant CV8 applicable to the User Role

8.1.4. DUIS Matrix

New User

The following User Role tables reflect the test Service Requests that must be executed by a new Party seeking to undertake UEPT, unless the Testing Participant has descoped a subset of Service Requests and this subset has been agreed with DCC or, where referred to the Panel, has been determined by the Panel. The tests are those indicated as ‘Mandatory, Mandatory SMETS1 and Mandatory SMETS2+’ in the CV column, for which they must be executed for each specific User Role. Those indicated as ‘Mandatory’ must be executed in respect of a SMETS1 Device and a SMETS2+ Device. Those indicated as ‘Mandatory SMETS1’ must be executed in respect of a SMETS1 Device. Those indicated as ‘Mandatory SMETS2+’ must be executed in respect of a SMETS2+ Device. Where the test Service Requests are indicated as N/A there is no requirement to test during execution of the test scenarios.

Additional SR Testing

Where a Party is seeking to become an Eligible User for Service Request(s) that they have not successfully previously completed UEPT for in that same User Role, then they must be executed where indicated by User Role and ‘Mandatory’, ‘Mandatory SMETS1’ or ‘Mandatory SMETS2+’ in the CV column in the table below. Those indicated as

‘Mandatory’ must be executed in respect of a SMETS1 Device and a SMETS2+ Device. Those indicated as ‘Mandatory SMETS1’ must be executed in respect of a SMETS1 Device. Those indicated as ‘Mandatory SMETS2+’ must be executed in respect of a SMETS2+ Device. Where the test Service Requests are indicated as N/A there is no requirement to test during execution of the test scenarios:

8.1.5. Import Supplier (IS) User Role

Service Reference	Service Reference Variant	Name	Critical	CV1 – On Demand	CV1 – Future Dated	CV2 – On Demand	CV3 – On Demand	CV4 – On Demand	CV5 – On Demand	CV5 – Future Dated	CV6 – On Demand	CV7 – On Demand	CV8 – DCC Only	IS
1.1	1.1.1	Update Import Tariff (Primary Element)	Y	N/A	N/A	N/A	N/A	Mandatory	Mandatory SMETS 2	N/A	N/A	N/A	N/A	IS
1.1	1.1.2	Update Import Tariff (Secondary Element)	Y	N/A	N/A	N/A	N/A	Mandatory SMETS 2	N/A	Mandatory SMETS 2	N/A	N/A	N/A	IS
1.2	1.2.1	Update Price (Primary Element)	Y	N/A	N/A	N/A	N/A	Mandatory	Mandatory SMETS 2	N/A	N/A	N/A	N/A	IS
1.2	1.2.2	Update Price (Secondary Element)	Y	N/A	N/A	N/A	N/A	Mandatory SMETS 2	N/A	Mandatory SMETS 2	N/A	N/A	N/A	IS
1.5	1.5	Update Meter Balance	Y	N/A	N/A	N/A	N/A	Mandatory	N/A	N/A	N/A	Mandatory SMETS 2	N/A	IS
1.6	1.6	Update Payment Mode	Y	N/A	N/A	N/A	N/A	Mandatory	N/A	Mandatory SMETS 2	N/A	N/A	N/A	IS
1.7	1.7	Reset Tariff Block Counter Matrix	Y	N/A	N/A	N/A	N/A	Mandatory SMETS 2	N/A	N/A	Mandatory SMETS 2	N/A	N/A	IS
2.1	2.1	Update Prepay Configuration	Y	N/A	N/A	N/A	N/A	Mandatory	Mandatory SMETS 2	N/A	N/A	N/A	N/A	IS
2.2	2.2	Top Up Device	N	Mandatory	N/A	N/A	Mandatory SMETS 2	N/A	N/A	N/A	N/A	N/A	N/A	IS
2.3	2.3	Update Debt	Y	N/A	N/A	N/A	N/A	Mandatory	Mandatory SMETS 2	N/A	N/A	N/A	N/A	IS
2.5	2.5	Activate Emergency Credit	Y	N/A	N/A	N/A	N/A	Mandatory	Mandatory SMETS 2	N/A	N/A	N/A	N/A	IS
3.1	3.1	Display Message	N	Mandatory SMETS 2	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	IS
3.2	3.2	Restrict Access For Change Of Tenancy	N	Mandatory	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	IS
3.3	3.3	Clear Event Log	N	Mandatory	N/A	Mandatory SMETS 2	N/A	N/A	N/A	N/A	N/A	N/A	N/A	IS
3.4	3.4	Update Supplier Name	N	N/A	N/A	N/A	Mandatory SMETS 2	N/A	N/A	N/A	N/A	N/A	N/A	IS
3.5	3.5	Disable Privacy PIN	N	Mandatory SMETS 2	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	IS
4.1	4.1.1	Read Instantaneous Import Registers	N	Mandatory	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	IS
4.1	4.1.2	Read Instantaneous Import TOU Matrices	N	Mandatory	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	IS

4.1	4.1.3	Read Instantaneous Import TOU With Blocks Matrices	N	Mandatory	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	IS
4.3	4.3	Read Instantaneous Prepay Values	N	Mandatory	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	IS
4.4	4.4.2	Retrieve Change Of Mode / Tariff Triggered Billing Data Log	N	Mandatory	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	IS
4.4	4.4.3	Retrieve Billing Calendar Triggered Billing Data Log	N	Mandatory	N/A	Mandatory SMETS 2	N/A	N/A	N/A	N/A	N/A	N/A	N/A	IS
4.4	4.4.4	Retrieve Billing Data Log (Payment Based Debt Payments)	N	Mandatory	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	IS
4.4	4.4.5	Retrieve Billing Data Log (Prepayment Credits)	N	Mandatory	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	IS
4.6	4.6.1	Retrieve Import Daily Read Log	N	Mandatory	N/A	Mandatory SMETS 2	N/A	N/A	N/A	N/A	N/A	N/A	N/A	IS
4.8	4.8.1	Read Active Import Profile Data	N	Mandatory	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	IS
4.8	4.8.2	Read Reactive Import Profile Data	N	Mandatory	N/A	Mandatory SMETS 2	N/A	N/A	N/A	N/A	N/A	N/A	N/A	IS
4.10	4.10	Read Network Data	N	Mandatory	N/A	N/A	Mandatory SMETS 2	N/A	N/A	N/A	N/A	N/A	N/A	IS
4.11	4.11.1	Read Tariff (Primary Element)	N	Mandatory	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	IS
4.11	4.11.2	Read Tariff (Secondary Element)	N	Mandatory SMETS 2	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	IS
4.12	4.12.1	Read Maximum Demand Import Registers	N	N/A	Mandatory SMETS 2	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	IS
4.13	4.13	Read Prepayment Configuration	N	Mandatory	N/A	N/A	Mandatory SMETS 2	N/A	N/A	N/A	N/A	N/A	N/A	IS
4.14	4.14	Read Prepayment Daily Read Log	N	Mandatory SMETS 2	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	IS
4.15	4.15	Read Load Limit Data	N	Mandatory	Mandatory	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	IS
4.16	4.16	Read Active Power Import	N	Mandatory	N/A	N/A	Mandatory SMETS 2	N/A	N/A	N/A	N/A	N/A	N/A	IS
4.17	4.17	Retrieve Daily Consumption Log	N	Mandatory SMETS 2	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	IS
4.18	4.18	Read Meter Balance	N	Mandatory	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	IS
5.1	5.1	Create Schedule	N	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	Mandatory	IS
5.2	5.2	Read Schedule	N	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	Mandatory	IS
5.3	5.3	Delete Schedule	N	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	Mandatory	IS
6.2	6.2.1	Read Device Configuration (Voltage)	N	Mandatory	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	IS

6.2	6.2.2	Read Device Configuration (Randomisation)	N	Mandatory SMETS 2	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	IS
6.2	6.2.3	Read Device Configuration (Billing Calendar)	N	Mandatory	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	IS
6.2	6.2.4	Read Device Configuration (Identity Exc MPxN)	N	Mandatory	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	IS
6.2	6.2.5	Read Device Configuration (Instantaneous Power Thresholds)	N	Mandatory	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	IS
6.2	6.2.7	Read Device Configuration (MPxN)	N	Mandatory SMETS 2	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	IS
6.2	6.2.9	Read Device Configuration (Payment Mode)	N	Mandatory	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	IS
6.2	6.2.10	Read Device Configuration (Event Alert Behaviours)	N	Mandatory SMETS 2	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	IS
6.4	6.4.1	Update Device Configuration (Load Limiting General Settings)	Y	N/A	N/A	N/A	N/A	Mandatory	Mandatory SMETS 2	N/A	N/A	N/A	N/A	IS
6.4	6.4.2	Update Device Configuration (Load Limiting Counter Reset)	N	Mandatory	N/A	Mandatory SMETS 2	N/A	N/A	N/A	N/A	N/A	N/A	N/A	IS
6.8	6.8	Update Device Configuration (Billing Calendar)	Y	N/A	N/A	N/A	N/A	Mandatory	Mandatory SMETS 2	N/A	N/A	N/A	N/A	IS
6.11	6.11	Synchronise Clock	Y	N/A	N/A	N/A	N/A	Mandatory	Mandatory SMETS 2	N/A	N/A	N/A	N/A	IS
6.12	6.12	Update Device Configuration (Instantaneous Power Threshold)	N	Mandatory	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	IS
6.13	6.13	Read Event Or Security Log	N	Mandatory	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	IS
6.14	6.14.1	Update Device Configuration (Auxiliary Load Control Description)	Y	N/A	N/A	N/A	N/A	Mandatory SMETS 2	Mandatory SMETS 2	N/A	N/A	N/A	N/A	IS
6.14	6.14.2	Update Device Configuration (Auxiliary Load Control Scheduler)	Y	N/A	N/A	N/A	N/A	Mandatory SMETS 2	N/A	Mandatory SMETS 2	N/A	N/A	N/A	IS
6.14	6.14.3	Update Device Configuration (Auxiliary Controller Scheduler)	Y	N/A	N/A	N/A	N/A	Mandatory SMETS 2	Mandatory SMETS 2	N/A	N/A	N/A	N/A	IS
6.15	6.15.1	Update Security Credentials (KRP)	Y	N/A	N/A	N/A	N/A	Mandatory	Mandatory SMETS 2	N/A	N/A	N/A	N/A	IS
6.15	6.15.2	Update Security Credentials (Device)	Y	N/A	N/A	N/A	N/A	Mandatory SMETS 2	Mandatory SMETS 2	N/A	N/A	N/A	N/A	IS
6.17	6.17	Issue Security Credentials	Y	N/A	N/A	N/A	N/A	Mandatory SMETS 2	Mandatory SMETS 2	N/A	N/A	N/A	N/A	IS

6.20	6.20.1	Set Device Configuration (Import MPxN)	N	Mandatory SMETS 2	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	IS
6.21	6.21	Request Handover Of DCC Controlled Device	N	Mandatory	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	IS
6.22	6.22	Configure Alert Behaviour	N	Mandatory SMETS 2	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	IS
6.23	6.23	Update Security Credentials (CoS)	N	N/A	Mandatory	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	IS
6.24	6.24.1	Retrieve Device Security Credentials (KRP)	N	Mandatory	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	IS
6.24	6.24.2	Retrieve Device Security Credentials (Device)	Y	N/A	N/A	N/A	N/A	Mandatory SMETS 2	Mandatory SMETS 2	N/A	N/A	N/A	N/A	IS
6.25	6.25	Set Electricity Supply Tamper State	Y	N/A	N/A	N/A	N/A	Mandatory	Mandatory SMETS 2	N/A	N/A	N/A	N/A	IS
6.26	6.26	Update Device Configuration (Daily Resetting Of Tariff Block Counter)	Y	N/A	N/A	N/A	N/A	Mandatory SMETS 2	Mandatory SMETS 2	N/A	N/A	N/A	N/A	IS
6.28	6.28	Set CHF Sub GHz Configuration	N	Mandatory SMETS 2	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	IS
6.29	6.29	Request CHF Sub GHz Channel Scan	N	Mandatory SMETS 2	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	IS
6.30	6.30	Read CHF Sub GHz Configuration	N	Mandatory SMETS 2	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	IS
6.31	6.31	Read CHF Sub GHz Channel	N	Mandatory SMETS 2	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	IS
6.32	6.32	Read CHF Sub GHz Channel Log	N	Mandatory SMETS 2	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	IS
7.1	7.1	Enable Supply	Y	N/A	N/A	N/A	N/A	Mandatory	Mandatory SMETS 2	N/A	N/A	N/A	N/A	IS
7.2	7.2	Disable Supply	Y	N/A	N/A	N/A	N/A	Mandatory	Mandatory SMETS 2	N/A	N/A	N/A	N/A	IS
7.3	7.3	Arm Supply	Y	N/A	N/A	N/A	N/A	Mandatory	Mandatory SMETS 2	N/A	N/A	N/A	N/A	IS
7.4	7.4	Read Supply Status	N	Mandatory	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	IS
7.5	7.5	Activate Auxiliary Load	Y	N/A	N/A	N/A	N/A	Mandatory SMETS 2	Mandatory SMETS 2	N/A	N/A	N/A	N/A	IS
7.6	7.6	Deactivate Auxiliary Load	Y	N/A	N/A	N/A	N/A	Mandatory SMETS 2	N/A	N/A	N/A	Mandatory SMETS 2	N/A	IS
7.7	7.7	Read Auxiliary Load Control Switch Data	N	Mandatory SMETS 2	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	IS
7.8	7.8	Reset Auxiliary Load	Y	N/A	N/A	N/A	N/A	Mandatory SMETS 2	Mandatory SMETS 2	N/A	N/A	N/A	N/A	IS
7.9	7.9	Add Auxiliary Load To Boost Button	N	N/A	Mandatory SMETS 2	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	IS

7.10	7.10	Remove Auxiliary Load From Boost Button	N	Mandatory SMETS 2	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	IS
7.11	7.11	Read Boost Button Details	N	N/A	Mandatory SMETS 2	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	IS
7.10	7.12	Set Randomised Offset Limit	Y	N/A	N/A	N/A	N/A	Mandatory SMETS 2	Mandatory SMETS 2	N/A	N/A	N/A	N/A	IS
7.13	7.13	Set Auxiliary Controller State	Y	N/A	N/A	N/A	N/A	Mandatory SMETS 2	Mandatory SMETS 2	N/A	N/A	N/A	N/A	IS
7.14	7.14	Read Auxiliary Controller Configuration Data	N	Mandatory SMETS 2	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	IS
7.15	7.15	Read Auxiliary Controller Operational Data	N	Mandatory SMETS 2	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	IS
8.1	8.1.1	Commission Device	Y	N/A	N/A	N/A	N/A	Mandatory	Mandatory SMETS 2	N/A	N/A	N/A	N/A	IS
8.2	8.2	Read Inventory	N	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	Mandatory	IS
8.3	8.3	Decommission Device	N	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	Mandatory	IS
8.4	8.4	Update Inventory	N	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	Mandatory	IS
8.7	8.7.1	Join Service (Critical)	Y	N/A	N/A	N/A	N/A	Mandatory	Mandatory SMETS 2	N/A	N/A	N/A	N/A	IS
8.7	8.7.2	Join Service (Non Critical)	N	Mandatory	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	IS
8.8	8.8.1	Unjoin Service (Critical)	Y	N/A	N/A	N/A	N/A	Mandatory	Mandatory SMETS 2	N/A	N/A	N/A	N/A	IS
8.8	8.8.2	Unjoin Service (Non Critical)	N	Mandatory	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	IS
8.9	8.9	Read Device Log	N	Mandatory	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	IS
8.11	8.11	Update HAN Device Log	N	Mandatory	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	IS
8.12	8.12.1	Restore HAN Device Log	N	N/A	N/A	Mandatory SMETS 2	N/A	N/A	N/A	N/A	N/A	N/A	N/A	IS
8.12	8.12.2	Restore Gas Proxy Function Device Log	N	Mandatory SMETS 2	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	IS
8.13	8.13	Return Local Command Response	N	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	Mandatory SMETS 2	IS
8.14	8.14.1	Communications Hub Status Update-Install Success	N	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	Mandatory SMETS 2	IS
8.14	8.14.2	Communications Hub Status Update-No SMWAN	N	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	Mandatory SMETS 2	IS
8.14	8.14.3	Communications Hub Status Update-Fault Return	N	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	Mandatory SMETS 2	IS

8.14	8.14.4	Communications Hub Status Update- No Fault Return	N	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	Mandatory SMETS 2	IS
11.1	11.1	Update Firmware	N	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	Mandatory	IS
11.2	11.2	Read Firmware Version	N	Mandatory	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	IS
11.3	11.3	Activate Firmware	Y	N/A	N/A	N/A	N/A	Mandatory	Mandatory SMETS 2	N/A	N/A	N/A	N/A	IS
11.4	11.4	Update PPMID Firmware	N	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	Mandatory SMETS 2	IS
12.1	12.1	Request WAN Matrix	N	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	Mandatory SMETS 2	IS
12.2	12.2	Device Pre-notification	N	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	Mandatory	IS
		Count of N/A		55	106	105	106	77	84	107	110	109	96	-
		Count of Mandatory		36	2	0	0	19	0	0	0	0	8	65
		Count of Mandatory SMETS 2		20	3	6	5	15	27	4	1	2	7	90
												Total Tests	155	

8.1.6. Gas Supplier (GS) User Role

Service Reference	Service Reference Variant	Name	Critical	CV1 – On Demand	CV1 – Future Dated	CV2 – On Demand	CV3 – On Demand	CV4 – On Demand	CV5 – On Demand	CV5 – Future Dated	CV6 – On Demand	CV7 – On Demand	CV8 – DCC Only	GS
1.1	1.1.1	Update Import Tariff (Primary Element)	Y	N/A	N/A	N/A	N/A	Mandatory	Mandatory SMETS 2	N/A	N/A	N/A	N/A	GS
1.2	1.2.1	Update Price (Primary Element)	Y	N/A	N/A	N/A	N/A	Mandatory	Mandatory SMETS 2	N/A	N/A	N/A	N/A	GS
1.5	1.5	Update Meter Balance	Y	N/A	N/A	N/A	N/A	Mandatory	N/A	N/A	N/A	Mandatory SMETS 2	N/A	GS
1.6	1.6	Update Payment Mode	Y	N/A	N/A	N/A	N/A	Mandatory	N/A	Mandatory SMETS 2	N/A	N/A	N/A	GS
2.1	2.1	Update Prepay Configuration	Y	N/A	N/A	N/A	N/A	Mandatory	Mandatory SMETS 2	N/A	N/A	N/A	N/A	GS
2.2	2.2	Top Up Device	N	Mandatory	N/A	Mandatory SMETS 2	N/A	N/A	N/A	N/A	N/A	N/A	N/A	GS
2.3	2.3	Update Debt	Y	N/A	N/A	N/A	N/A	Mandatory	Mandatory SMETS 2	N/A	N/A	N/A	N/A	GS
2.5	2.5	Activate Emergency Credit	Y	N/A	N/A	N/A	N/A	Mandatory	Mandatory SMETS 2	N/A	N/A	N/A	N/A	GS
3.1	3.1	Display Message	N	Mandatory SMETS 2	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	GS

3.2	3.2	Restrict Access For Change Of Tenancy	N	Mandatory	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	GS
3.3	3.3	Clear Event Log	N	Mandatory	N/A	Mandatory SMETS 2	N/A	N/A	N/A	N/A	N/A	N/A	N/A	GS
3.4	3.4	Update Supplier Name	N	N/A	N/A	N/A	Mandatory SMETS 2	N/A	N/A	N/A	N/A	N/A	N/A	GS
3.5	3.5	Disable Privacy PIN	N	Mandatory SMETS 2	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	GS
4.1	4.1.1	Read Instantaneous Import Registers	N	Mandatory	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	GS
4.1	4.1.2	Read Instantaneous Import TOU Matrices	N	Mandatory	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	GS
4.1	4.1.4	Read Instantaneous Import Block Counters	N	Mandatory	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	GS
4.3	4.3	Read Instantaneous Prepay Values	N	Mandatory	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	GS
4.4	4.4.2	Retrieve Change Of Mode / Tariff Triggered Billing Data Log	N	Mandatory	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	GS
4.4	4.4.3	Retrieve Billing Calendar Triggered Billing Data Log	N	Mandatory	N/A	Mandatory SMETS 2	N/A	N/A	N/A	N/A	N/A	N/A	N/A	GS
4.4	4.4.4	Retrieve Billing Data Log (Payment Based Debt Payments)	N	Mandatory	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	GS
4.4	4.4.5	Retrieve Billing Data Log (Prepayment Credits)	N	Mandatory	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	GS
4.6	4.6.1	Retrieve Import Daily Read Log	N	Mandatory	N/A	Mandatory SMETS 2	N/A	N/A	N/A	N/A	N/A	N/A	N/A	GS
4.8	4.8.1	Read Active Import Profile Data	N	Mandatory	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	GS
4.10	4.10	Read Network Data	N	Mandatory	N/A	N/A	Mandatory SMETS 2	N/A	N/A	N/A	N/A	N/A	N/A	GS
4.11	4.11.1	Read Tariff (Primary Element)	N	Mandatory	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	GS
4.13	4.13	Read Prepayment	N	Mandatory	N/A	N/A	Mandatory SMETS 2	N/A	N/A	N/A	N/A	N/A	N/A	GS

		Configuration												
4.14	4.14	Read Prepayment Daily Read Log	N	Mandatory SMETS 2	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	GS
4.17	4.17	Retrieve Daily Consumption Log	N	Mandatory SMETS 2	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	GS
4.18	4.18	Read Meter Balance	N	Mandatory	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	GS
5.1	5.1	Create Schedule	N	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	Mandatory	GS
5.2	5.2	Read Schedule	N	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	Mandatory	GS
5.3	5.3	Delete Schedule	N	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	Mandatory	GS
6.2	6.2.3	Read Device Configuration (Billing Calendar)	N	Mandatory	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	GS
6.2	6.2.4	Read Device Configuration (Identity Exc MPxN)	N	Mandatory	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	GS
6.2	6.2.7	Read Device Configuration (MPxN)	N	Mandatory SMETS 2	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	GS
6.2	6.2.8	Read Device Configuration (Gas)	N	Mandatory	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	GS
6.2	6.2.9	Read Device Configuration (Payment Mode)	N	Mandatory	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	GS
6.2	6.2.10	Read Device Configuration (Event Alert Behaviours)	N	Mandatory SMETS 2	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	GS
6.6	6.6	Update Device Configuration (Gas Conversion)	Y	N/A	N/A	N/A	N/A	Mandatory	N/A	N/A	N/A	N/A	N/A	GS
6.7	6.7	Update Device Configuration (Gas Flow)	Y	N/A	N/A	N/A	N/A	Mandatory	N/A	N/A	N/A	N/A	N/A	GS
6.8	6.8	Update Device Configuration (Billing Calendar)	Y	N/A	N/A	N/A	N/A	Mandatory	Mandatory SMETS 2	N/A	N/A	N/A	N/A	GS
6.11	6.11	Synchronise Clock	Y	N/A	N/A	N/A	N/A	Mandatory	Mandatory SMETS 2	N/A	N/A	N/A	N/A	GS
6.13	6.13	Read Event Or Security Log	N	Mandatory	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	GS

6.15	6.15.1	Update Security Credentials (KRP)	Y	N/A	N/A	N/A	N/A	Mandatory	Mandatory SMETS 2	N/A	N/A	N/A	N/A	GS
6.15	6.15.2	Update Security Credentials (Device)	Y	N/A	N/A	N/A	N/A	Mandatory SMETS 2	Mandatory SMETS 2	N/A	N/A	N/A	N/A	GS
6.17	6.17	Issue Security Credentials	Y	N/A	N/A	N/A	N/A	Mandatory SMETS 2	Mandatory SMETS 2	N/A	N/A	N/A	N/A	GS
6.20	6.20.1	Set Device Configuration (Import MPxN)	N	Mandatory SMETS 2	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	GS
6.21	6.21	Request Handover Of DCC Controlled Device	N	Mandatory	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	GS
6.22	6.22	Configure Alert Behaviour	N	Mandatory SMETS 2	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	GS
6.23	6.23	Update Security Credentials (CoS)	N	N/A	Mandatory	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	GS
6.24	6.24.1	Retrieve Device Security Credentials (KRP)	N	Mandatory	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	GS
6.24	6.24.2	Retrieve Device Security Credentials (Device)	Y	N/A	N/A	N/A	N/A	Mandatory SMETS 2	Mandatory SMETS 2	N/A	N/A	N/A	N/A	GS
6.28	6.28	Set CHF Sub GHz Configuration	N	Mandatory SMETS 2	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	GS
6.29	6.29	Request CHF Sub GHz Channel Scan	N	Mandatory SMETS 2	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	GS
6.30	6.30	Read CHF Sub GHz Configuration	N	Mandatory SMETS 2	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	GS
6.31	6.31	Read CHF Sub GHz Channel	N	Mandatory SMETS 2	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	GS
6.32	6.32	Read CHF Sub GHz Channel Log	N	Mandatory SMETS 2	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	GS
7.2	7.2	Disable Supply	Y	N/A	N/A	N/A	N/A	Mandatory	Mandatory SMETS 2	N/A	N/A	N/A	N/A	GS
7.3	7.3	Arm Supply	Y	N/A	N/A	N/A	N/A	Mandatory	Mandatory SMETS 2	N/A	N/A	N/A	N/A	GS
7.4	7.4	Read Supply Status	N	Mandatory	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	GS

8.1	8.1.1	Commission Device	Y	N/A	N/A	N/A	N/A	Mandatory	Mandatory SMETS 2	N/A	N/A	N/A	N/A	GS
8.2	8.2	Read Inventory	N	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	Mandatory	GS
8.3	8.3	Decommission Device	N	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	Mandatory	GS
8.4	8.4	Update Inventory	N	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	Mandatory	GS
8.7	8.7.1	Join Service (Critical)	Y	N/A	N/A	N/A	N/A	Mandatory	Mandatory SMETS 2	N/A	N/A	N/A	N/A	GS
8.7	8.7.2	Join Service (Non Critical)	N	Mandatory	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	GS
8.8	8.8.1	Unjoin Service (Critical)	Y	N/A	N/A	N/A	N/A	Mandatory	Mandatory SMETS 2	N/A	N/A	N/A	N/A	GS
8.8	8.8.2	Unjoin Service (Non Critical)	N	Mandatory	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	GS
8.9	8.9	Read Device Log	N	Mandatory	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	GS
8.11	8.11	Update HAN Device Log	N	Mandatory	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	GS
8.12	8.12.1	Restore HAN Device Log	N	N/A	N/A	Mandatory SMETS 2	N/A	N/A	N/A	N/A	N/A	N/A	N/A	GS
8.12	8.12.2	Restore Gas Proxy Function Device Log	N	Mandatory SMETS 2	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	GS
8.13	8.13	**Return** Local Command Response	N	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	Mandatory SMETS 2	GS
8.14	8.14.1	Communications Hub Status Update-Install Success	N	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	Mandatory SMETS 2	GS
8.14	8.14.2	Communications Hub Status Update-	N	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	Mandatory SMETS 2	GS
8.14	8.14.3	Communications Hub Status Update-Fault Return	N	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	Mandatory SMETS 2	GS
8.14	8.14.4	Communications Hub Status Update- No Fault Return	N	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	Mandatory SMETS 2	GS
11.1	11.1	Update Firmware	N	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	Mandatory	GS
11.2	11.2	Read Firmware Version	N	Mandatory	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	GS

11.3	11.3	Activate Firmware	Y	N/A	N/A	N/A	N/A	Mandatory	Mandatory SMETS 2	N/A	N/A	N/A	N/A	GS
11.4	11.4	Update PPMID Firmware	N	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	Mandatory SMETS 2	GS
12.1	12.1	Request WAN Matrix	N	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	Mandatory SMETS 2	GS
12.2	12.2	Device Pre-notification	N	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	Mandatory	GS
		Count of N/A		39	82	78	80	62	66	82	83	82	68	-
		Count of Mandatory		30	1	0	0	18	0	0	0	0	8	57
		Count of Mandatory SMETS 2		14	0	5	3	3	17	1	0	1	7	51
												Total Tests		108

8.1.7. Export Supplier (ES) User Role

Service Reference	**Service Reference Variant**	**Name**	**Critical**	**CV1 – On Demand**	**CV1 – Future Dated**	**CV2 – On Demand**	**CV3 – On Demand**	**CV4 – On Demand**	**CV5 – On Demand**	**CV5 – Future Dated**	**CV6 – On Demand**	**CV7 – On Demand**	**CV8 – DCC Only**	**ES**
4.2	4.2	Read Instantaneous Export Registers	N	Mandatory	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	ES
4.6	4.6.2	Retrieve Export Daily Read Log	N	Mandatory SMETS 2	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	ES
4.8	4.8.3	Read Export Profile Data	N	Mandatory	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	ES
4.12	4.12.2	Read Maximum Demand Export Registers	N	Mandatory SMETS 2	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	ES
5.1	5.1	Create Schedule	N	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	Mandatory	ES
5.2	5.2	Read Schedule	N	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	Mandatory	ES
5.3	5.3	Delete Schedule	N	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	Mandatory	ES
6.2	6.2.4	Read Device Configuration (Identity Exc MPxN)	N	Mandatory	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	ES
6.2	6.2.7	Read Device Configuration (MPxN)	N	Mandatory SMETS 2	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	ES
6.2	6.20.2	Set Device Configuration (Export MPAN)	N	Mandatory SMETS 2	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	ES
7.4	7.4	Read Supply Status	N	Mandatory	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	ES
8.2	8.2	Read Inventory	N	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	Mandatory	ES
8.4	8.4	Update Inventory	N	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	Mandatory	ES

11.2	11.2	Read Firmware Version	N	Mandatory	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	ES
12.1	12.1	Request WAN Matrix	N	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	Mandatory SMETS 2	ES
12.2	12.2	Device Pre-notification	N	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	Mandatory	ES
		Count of N/A		7	16	16	16	16	16	16	16	16	9	-
		Count of Mandatory		5	0	0	0	0	0	0	0	0	6	11
		Count of Mandatory SMETS 2		4	0	0	0	0	0	0	0	0	1	5
													Total Tests	16

8.1.8. Electricity Distributor (ED) User Role

Service Reference	Service Reference Variant	Name	Critical	CV1 – On Demand	CV1 – Future Dated	CV2 – On Demand	CV3 – On Demand	CV4 – On Demand	CV5 – On Demand	CV5 – Future Dated	CV6 – On Demand	CV7 – On Demand	CV8 – DCC Only	ED
4.1	4.1.1	Read Instantaneous Import Registers	N	Mandatory	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	ED
4.1	4.1.2	Read Instantaneous Import TOU Matrices	N	Mandatory	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	ED
4.1	4.1.3	Read Instantaneous Import TOU With Blocks Matrices	N	Mandatory	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	ED
4.2	4.2	Read Instantaneous Export Registers	N	Mandatory	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	ED
4.8	4.8.1	Read Active Import Profile Data	N	Mandatory	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	ED
4.8	4.8.2	Read Reactive Import Profile Data	N	Mandatory	N/A	Mandatory SMETS 2	N/A	N/A	N/A	N/A	N/A	N/A	N/A	ED
4.8	4.8.3	Read Export Profile Data	N	Mandatory	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	ED
4.10	4.10	Read Network Data	N	Mandatory	N/A	N/A	Mandatory SMETS 2	N/A	N/A	N/A	N/A	N/A	N/A	ED
4.12	4.12.1	Read Maximum Demand Import Registers	N	N/A	Mandatory SMETS 2	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	ED
4.12	4.12.2	Read Maximum Demand Export Registers	N	N/A	Mandatory SMETS 2	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	ED
4.15	4.15	Read Load Limit Data	N	Mandatory	Mandatory SMETS 2	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	ED
4.16	4.16	Read Active Power Import	N	Mandatory	N/A	N/A	Mandatory SMETS 2	N/A	N/A	N/A	N/A	N/A	N/A	ED

4.17	4.17	Retrieve Daily Consumption Log	N	Mandatory SMETS 2	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	ED
5.1	5.1	Create Schedule	N	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	Mandatory	ED
5.2	5.2	Read Schedule	N	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	Mandatory	ED
5.3	5.3	Delete Schedule	N	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	Mandatory	ED
6.2	6.2.1	Read Device Configuration (Voltage)	N	Mandatory	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	ED
6.2	6.2.2	Read Device Configuration (Randomisation)	N	Mandatory SMETS 2	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	ED
6.2	6.2.4	Read Device Configuration (Identity Exc MPxN)	N	Mandatory	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	ED
6.2	6.2.7	Read Device Configuration (MPxN)	N	Mandatory SMETS 2	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	ED
6.2	6.2.10	Read Device Configuration (Event Alert Behaviours)	N	Mandatory SMETS 2	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	ED
6.5	6.5	Update Device Configuration (Voltage)	N	Mandatory	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	ED
6.13	6.13	Read Event Or Security Log	N	Mandatory	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	ED
6.15	6.15.1	Update Security Credentials (KRP)	Y	N/A	N/A	N/A	N/A	Mandatory	Mandatory SMETS 2	N/A	N/A	N/A	N/A	ED
6.18	6.18.1	Set Maximum Demand Configurable Time Period	N	Mandatory SMETS 2	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	ED
6.18	6.18.2	Reset Maximum Demand Registers	N	Mandatory SMETS 2	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	ED
6.22	6.22	Configure Alert Behaviour	N	Mandatory SMETS 2	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	ED
6.24	6.24.1	Retrieve Device Security Credentials (KRP)	N	Mandatory	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	ED
6.27	6.27	Update Device Configuration (Daily Resetting Of Tariff Block Counter)	N	Mandatory SMETS 2	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	ED
7.4	7.4	Read Supply Status	N	Mandatory	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	ED
7.7	7.7	Read Auxiliary Load Control Switch Data	N	Mandatory SMETS 2	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	ED

7.14	7.14	Read Auxiliary Controller Configuration Data	N	Mandatory SMETS 2	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	ED
7.15	7.15	Read Auxiliary Controller Operational Data	N	Mandatory SMETS 2	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	ED
8.2	8.2	Read Inventory	N	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	Mandatory	ED
8.4	8.4	Update Inventory	N	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	Mandatory	ED
11.2	11.2	Read Firmware Version	N	Mandatory	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	ED
12.1	12.1	Request WAN Matrix	N	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	Mandatory SMETS 2	ED
12.2	12.2	Device Pre-notification	N	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	Mandatory	ED
		Count of N/A		10	35	37	36	37	37	38	38	38	31	-
		Count of Mandatory		17	0	0	0	1	0	0	0	0	6	24
		Count of Mandatory SMETS 2		11	3	1	2	0	1	0	0	0	1	19
												Total Tests		43

8.1.9. Gas Transporter (GT) User Role

Service Reference	Service Reference Variant	Name	Critical	CV1 – On Demand	CV1 – Future Dated	CV2 – On Demand	CV3 – On Demand	CV4 – On Demand	CV5 – On Demand	CV5 – Future Dated	CV6 – On Demand	CV7 – On Demand	CV8 – DCC Only	GT
4.1	4.1.1	Read Instantaneous Import Registers	N	Mandatory	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	GT
4.1	4.1.2	Read Instantaneous Import TOU Matrices	N	Mandatory	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	GT
4.8	4.8.1	Read Active Import Profile Data	N	Mandatory	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	GT
4.10	4.10	Read Network Data	N	Mandatory	N/A	N/A	Mandatory SMETS 2	N/A	N/A	N/A	N/A	N/A	N/A	GT
4.17	4.17	Retrieve Daily Consumption Log	N	Mandatory SMETS 2	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	GT
5.1	5.1	Create Schedule	N	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	Mandatory	GT
5.2	5.2	Read Schedule	N	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	Mandatory	GT
5.3	5.3	Delete Schedule	N	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	Mandatory	GT
6.2	6.2.4	Read Device Configuration (Identity Exc MPxN)	N	Mandatory	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	GT
6.2	6.2.7	Read Device Configuration (MPxN)	N	Mandatory SMETS 2	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	GT

6.2	6.2.8	Read Device Configuration (Gas)	N	Mandatory	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	GT
6.13	6.13	Read Event Or Security Log	N	Mandatory	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	GT
6.15	6.15.1	Update Security Credentials (KRP)	Y	N/A	N/A	N/A	N/A	Mandatory	Mandatory SMETS 2	N/A	N/A	N/A	N/A	GT
6.24	6.24.1	Retrieve Device Security Credentials (KRP)	N	Mandatory	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	GT
7.4	7.4	Read Supply Status	N	Mandatory	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	GT
8.2	8.2	Read Inventory	N	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	Mandatory	GT
8.4	8.4	Update Inventory	N	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	Mandatory	GT
11.2	11.2	Read Firmware Version	N	Mandatory	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	GT
12.1	12.1	Request WAN Matrix	N	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	Mandatory SMETS 2	GT
12.2	12.2	Device Pre-notification	N	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	Mandatory	GT
14.1	14.1	Record Network Data (GAS)	N	Mandatory SMETS 2	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	GT
		Count of N/A	-	8	21	21	20	20	20	21	21	21	14	-
		Count of Mandatory	-	10	0	0	0	1	0	0	0	0	6	17
		Count of Mandatory SMETS 2	-	3	0	0	1	0	1	0	0	0	1	6
												Total Tests		23

8.1.10. Registered Supplier Agent (RSA) User Role

Service Reference	Service Reference Variant	Name	Critical	CV1 – On Demand	CV1 – Future Dated	CV2 – On Demand	CV3 – On Demand	CV4 – On Demand	CV5 – On Demand	CV5 – Future Dated	CV6 – On Demand	CV7 – On Demand	CV8 – DCC Only	RSA
6.2	**6.2.1**	**Read Device Configuration (Voltage)**	**N**	**Mandatory**	**N/A**	**N/A**	**N/A**	**N/A**	**N/A**	**N/A**	**N/A**	**N/A**	**N/A**	**RSA**
6.2	**6.2.2**	**Read Device Configuration (Randomisation)**	**N**	**Mandatory SMETS 2**	**N/A**	**N/A**	**N/A**	**N/A**	**N/A**	**N/A**	**N/A**	**N/A**	**N/A**	**RSA**
6.2	**6.2.3**	**Read Device Configuration (Billing Calendar)**	**N**	**Mandatory**	**N/A**	**N/A**	**N/A**	**N/A**	**N/A**	**N/A**	**N/A**	**N/A**	**N/A**	**RSA**
6.2	**6.2.4**	**Read Device Configuration (Identity Exc MPxN)**	**N**	**Mandatory**	**N/A**	**N/A**	**N/A**	**N/A**	**N/A**	**N/A**	**N/A**	**N/A**	**N/A**	**RSA**
6.2	**6.2.5**	**Read Device Configuration**	**N**	**Mandatory**	**N/A**	**N/A**	**N/A**	**N/A**	**N/A**	**N/A**	**N/A**	**N/A**	**N/A**	**RSA**

		(Instantaneous Power Thresholds)												
6.2	6.2.7	Read Device Configuration (MPxN)	N	Mandatory SMETS 2	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	RSA
6.2	6.2.8	Read Device Configuration (Gas)	N	Mandatory	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	RSA
6.2	6.2.9	Read Device Configuration (Payment Mode)	N	Mandatory	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	RSA
6.13	6.13	Read Event Or Security Log	N	Mandatory	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	RSA
6.3	6.3	Read CHF Sub GHz Configuration	N	Mandatory SMETS 2	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	RSA
6.31	6.31	Read CHF Sub GHz Channel	N	Mandatory SMETS 2	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	RSA
6.32	6.32	Read CHF Sub GHz Channel Log	N	Mandatory SMETS 2	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	RSA
7.4	7.4	Read Supply Status	N	Mandatory	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	RSA
8.2	8.2	Read Inventory	N	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	Mandatory	RSA
8.4	8.4	Update Inventory	N	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	Mandatory	RSA
8.14	8.14.3	Communications Hub Status Update-Fault Return	N	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	Mandatory SMETS 2	RSA
8.14	8.14.3	Communications Hub Status Update-No Fault Returned	N	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	Mandatory SMETS 2	RSA
11.2	11.2	Read Firmware Version	N	Mandatory	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	RSA
12.1	12.1	Request WAN Matrix	N	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	Mandatory SMETS 2	RSA
12.2	12.2	Device Pre-notification	N	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	Mandatory	RSA
		Count of N/A	-	6	20	20	20	20	20	20	20	20	14	-
		Count of Mandatory	-	9	0	0	0	0	0	0	0	0	3	12
		Count of Mandatory SMETS 2	-	5	0	0	0	0	0	0	0	0	3	8
												Total Tests		20

8.1.10A. Meter Data Retriever (MDR) User Role

Service Reference	Service Reference Variant	Name	Critical	CV1 – On Demand	CV1 – Future Dated	CV2 – On Demand	CV3 – On Demand	CV4 – On Demand	CV5 – On Demand	CV5 – Future Dated	CV6 – On Demand	CV7 – On Demand	CV8 – DCC Only	MDR
4.1	4.1.1	Read Instantaneous Import Registers	N	Mandatory	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	MDR
4.2	4.2	Read Instantaneo	N	Mandatory	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	MDR

		us Export Register Values												
4.6	4.6.1	Retrieve Import Daily Read Log	N	Mandatory	N/A	Mandatory SMETS 2	N/A	N/A	N/A	N/A	N/A	N/A	N/A	MDR
4.6	4.6.2	Retrieve Export Daily Read Log	N	Mandatory SMETS 2	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	MDR
4.8	4.8.1	Read Active Import Profile Data	N	Mandatory	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	MDR
4.8	4.8.3	Read Export Profile Data	N	Mandatory	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	MDR
4.17	4.17	Retrieve Daily Consumption Log	N	Mandatory SMETS 2	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	MDR
5.1	5.1	Create Schedule	N	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	Mandatory	MDR
5.2	5.2	Read Schedule	N	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	Mandatory	MDR
5.3	5.3	Delete Schedule	N	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	Mandatory	MDR
8.2	8.2	Read Inventory	N	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	Mandatory	MDR
		Count of N/A	-	4	11	10	11	11	11	11	11	11	7	-
		Count of Mandatory	-	5	0	0	0	0	0	0	0	0	4	9
		Count of Mandatory SMETS 2	-	2	0	1	0	0	0	0	0	0	0	3
												Total Tests		12

8.1.11. Registered Supplier Agent (RSA) User Role

Service Reference	Service Reference Variant	Name	Critical	CV1 – On Demand	CV1 – Future Dated	CV2 – On Demand	CV3 – On Demand	CV4 – On Demand	CV5 – On Demand	CV5 – Future Dated	CV6 – On Demand	CV7 – On Demand	CV8 – DCC Only	OU
4.8	4.8.1	Read Active Import Profile Data	N	Mandatory	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	OU
4.8	4.8.2	Read Reactive Import Profile Data	N	Mandatory	N/A	Mandatory SMETS 2	N/A	N/A	N/A	N/A	N/A	N/A	N/A	OU
4.8	4.8.3	Read Export Profile Data	N	N/A	Mandatory	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	OU
4.11	4.11.1	Read Tariff (Primary Element)	N	Mandatory	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	OU
4.11	4.11.2	Read Tariff (Secondary Element)	N	Mandatory SMETS 2	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	OU

4.17	4.17	Retrieve Daily Consumption Log	N	Mandatory SMETS 2	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	OU
5.1	5.1	Create Schedule	N	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	Mandatory	OU
5.2	5.2	Read Schedule	N	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	Mandatory	OU
5.3	5.3	Delete Schedule	N	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	Mandatory	OU
6.2	6.2.4	Read Device Configuration (Identity Exc MPxN)	N	Mandatory	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	OU
6.2	6.2.7	Read Device Configuration (MPxN)	N	Mandatory SMETS 2	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	OU
7.7	7.7	Read Auxiliary Load Control Switch Data	N	Mandatory SMETS 2	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	OU
7.11	7.11	Read Boost Button Details	N	N/A	Mandatory SMETS 2	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	OU
7.14	7.14	Read Auxiliary Controller Configuration Data	N	Mandatory SMETS 2	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	OU
7.15	7.15	Read Auxiliary Controller Operational Data	N	Mandatory SMETS 2	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	OU
8.2	8.2	Read Inventory	N	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	Mandatory	OU
8.4	8.4	Update Inventory	N	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	Mandatory	OU
8.7	8.7.2	Join Service (Non Critical)	N	Mandatory	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	OU
8.8	8.8.2	Unjoin Service (Non Critical)	N	Mandatory	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	OU
8.9	8.9	Read Device Log	N	Mandatory	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	OU
8.11	8.11	Update HAN Device Log	N	Mandatory	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	OU
9.1	9.1	Request Customer Identification Number	N	Mandatory SMETS 2	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	OU
11.2	11.2	Read Firmware Version	N	Mandatory	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	OU
12.1	12.1	Request WAN Matrix	N	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	Mandatory	OU

													SMETS 2	
12.2	12.2	Device Pre-notification	N	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	Mandatory	OU
		Count of N/A	-	9	224	224	25	25	25	25	25	25	18	-
		Count of Mandatory	-	9	0	0	0	0	0	0	0	0	6	15
		Count of Mandatory SMETS 2	-	7	1	1	0	0	0	0	0	0	1	10
												Total Tests		25

8.1.12. Device Alert Tests

The following table outlines the Device Alert tests required to be executed by User Role. The purpose of these tests is to prove that a party can receive a subset of Device Alerts based on the differing types of Alerts that can be received.

New User

The following User Role tables reflect the Device Alerts that must be executed by a new Party seeking to undertake UEPT, unless the Testing Participant has descoped a subset of Device Alert Tests and this has been agreed with DCC or, where referred to the Panel, has been determined by the Panel. The tests are those indicated as 'Mandatory, Mandatory SMETS1 and Mandatory SMETS2+ ' in the test scenario column, for which they must be executed for each specific User Role. Those indicated as 'Mandatory' must be executed in respect of a SMETS1 Device and a SMETS2+ Device. Those indicated as 'Mandatory SMETS1' must be executed in respect of a SMETS1 Device. Those indicated as 'Mandatory SMETS2+' must be executed in respect of a SMETS2+ Device. Where the Device Alert tests are indicated as N/A there is no requirement to test during execution of the test scenarios.

8.1.13. Device Alert Tests – IS

Event / Alert Code	Event / Alert Code Meaning	Device Alert Variant	Critical	Test Scenario	User Role
0x8F32**	Supply Armed	Device Alert – Type 1 (Alert Code and Timestamp) DLMS	Y	Mandatory	IS
0x8183	Device joined SMHAN	Device Alert – Type 1 (Alert Code and Timestamp) DLMS	N	Mandatory SMETS2+	IS
0x8F66	Future – date HAN Interface Command Successfully Actioned	Device Alert – Type 2 (Alert Code, Timestamp and Specific Data) DLMS	Y	Mandatory SMETS2+	IS

**Where the Device being used in testing is not able to support the generation of this Alert, the DCC shall notify the Testing Participant of a different Alert that needs to be tested.

8.1.14. Device Alert Tests – GS

Event / Alert Code	Event / Alert Code Meaning	Device Alert Variant	Critical	Test Scenario	User Role
0x8F32**	Supply Armed	Device Alert – Type 1 (Alert Code and Timestamp) Zigbee	Y	Mandatory	GS
0x8183	Device joined SMHAN	Device Alert – Type 1 (Alert Code and Timestamp) Zigbee	N	Mandatory SMETS2+	GS
0x8F66	Future – date HAN Interface Command Successfully Actioned	Device Alert – Type 2 (Alert Code, Timestamp and -Specific Data) Zigbee	Y	Mandatory SMETS2+	-GS

**Where the Device being used in testing is not able to support the generation of this Alert, the DCC shall notify the Testing Participant of a different Alert that needs to be tested.

8.1.15. Device Alert Tests – ES

Event / Alert Code	Event / Alert Code Meaning	Device Alert Variant	Critical	CTS Test Scenario	User Role
No alerts identified from Device to Export Supplier					

8.1.16. Device Alert Tests – ED

Event / Alert Code	Event / Alert Code Meaning	Device Alert Variant	Critical	Test Scenario	User Role
0x8002	Average RMS Voltage above Average RMS Over Voltage Threshold (current value above threshold; previous value below threshold)	Device Alert – Type 1 (Alert Code and Timestamp) DLMS	N	Mandatory SMETS2+	-ED
0x8F35	Supply Outage Restored	Device Alert – Type 2 (Alert Code, Timestamp and Specific Data) DLMS	Y	Mandatory SMETS2+	ED
0x8F36	Supply Outage Restored - Outage >= 3 minutes	Device Alert – Type 2 (Alert Code, Timestamp and Specific Data) DLMS	Y	Mandatory SMETS2+	ED
0x8F40	Average RMS Voltage above Average RMS Over Voltage Threshold (current value above threshold; previous value below threshold)	Device Alert – Type 1 (Alert Code and Timestamp) DLMS	N	Mandatory SMETS1	-ED
0x8F411	SMETS1 Average RMS Voltage below Average RMS Under Voltage Threshold	Device Alert – Type 1 (Alert Code and Timestamp) DLMS	N	Mandatory SMETS1	ED

	(current value below threshold; previous value above threshold)				

8.1.17. Device Alert Tests – GT

Event / Alert Code	Event / Alert Code Meaning	Device Alert Variant	Critical	Test Scenario	User Role
No alerts identified from Device to Gas Transporter					

8.1.18. DCC Alert Tests

The following table outlines the DCC Alert tests required to be executed by User Role. The purpose of these tests is to prove that a party can receive a subset of DCC Alerts based on the differing types of Alerts that can be received.

New User

The following User Role tables reflect the DCC Alert Tests that must be executed by a new Party seeking to undertake UEPT unless the Testing Participant has descoped a subset of DCC Alert Tests and this have been agreed with DCC or, where referred to the Panel, has been determined by the Panel. The tests are those indicated as ‘Mandatory, Mandatory SMETS1 and Mandatory SMETS2+‘ in the test scenario column, for which they must be executed for each specific User Role. Those indicated as ‘Mandatory’ must be executed in respect of a SMETS1 Device and a SMETS2+ Device. Those indicated as ‘Mandatory SMETS1’ must be executed in respect of a SMETS1 Device. Those indicated as ‘Mandatory SMETS2+’ must be executed in respect of a SMETS2+ Device. Where the DCC Alert Tests are indicated as N/A there is no requirement to test during execution of the test scenarios.

The Alerts highlighted in Blue are Device Alert Tests to be executed against Dual Band Communications Hub by User Role.

8.1.19. DCC Alert Tests – IS

Reference	Name	Test Scenario	Applicable User Role
N17	DSP Schedule Removal – Schedule removal due to Change of Supplier	Mandatory	Previously Registered IS
N24	Update HAN Device Log Result – Successful Communications Hub Function Whitelist Update	Mandatory SMETS2+	IS
N27	Change of Supplier – Device Change of Supplier	Mandatory	Previously Registered IS
N49, N50, N51, N52	Firmware Version Mismatch	Optional	IS
N53	Command Not Delivered To ESME	Mandatory SMETS2+	IS
N54	Dual Band CH Sub GHz Alert	Mandatory SMETS2+	IS

N55	SMETS1 Service Provider Alert	Mandatory SMETS1	IS
N56	SMETS1 Service Provider Provision of prepayment top-up UTRN	Mandatory SMETS1	IS

8.1.20. DCC Alert Tests – GS

Reference	Name	Test Scenario	Applicable User Role
N17	DSP Schedule Removal – Schedule removal due to Change of Supplier	Mandatory	Previously Registered GS
N24	Update HAN Device Log Result – Successful Communications Hub Function Whitelist Update	Mandatory SMETS2+	GS
N27	Change of Supplier – Device Change of Supplier	Mandatory SMETS2+	Previously Registered GS
N49, N50, N51, N52	Firmware Version Mismatch	Optional SMETS2+	GS
N54	Dual Band CH Sub GHz Alert	Mandatory SMETS2+	GS
N55	SMETS1 Service Provider Alert	Mandatory SMETS1	GS
N56	SMETS1 Service Provider Provision of prepayment top-up UTRN	Mandatory SMETS1	GS
N57	SMETS1 CH Firmware notification	Mandatory SMETS1	GS

8.1.21. DCC Alert Tests – ES

Reference	Name	CTS Test Scenario	Applicable User Role
N1	Device Status Change – Electricity Smart Meter Decommission or Withdrawal	Mandatory SMETS2+	Registered ES
N55	SMETS1 Service Provider Alert	Mandatory SMETS1	Registered ES

8.1.22. DCC Alert Tests – ED

Reference	Name	Test Scenario	Applicable User Role
AD1	Power Outage Event	Mandatory SMETS2+	Registered ED

N1	Device Status Change – Electricity Smart Meter Decommission or Withdrawal	Mandatory SMETS2+	Registered ED
N16	Device Identity Confirmation	Mandatory SMETS2+	Registered ED
N53	Command Not Delivered To ESME	Mandatory SMETS2+	Registered ED
N55	SMETS1 Service Provider Alert	Mandatory SMETS1	Registered ED

8.1.23. DCC Alert Tests – GT

Reference	Name	Test Scenario	Applicable User Role
AD1	Power Outage Event	Mandatory SMETS2+	Registered GT
N2	Device Status Change - Gas Smart Meter Decommission or Withdrawal	Mandatory SMETS2+	Registered GT
N16	Device Identity Confirmation	Mandatory SMETS2+	Registered GT
N55	SMETS1 Service Provider Alert	Mandatory SMETS1	Registered GT

8.1.24. DCC Alert Tests - RSA

Reference	Name	Test Scenario	Applicable User Role
N55	SMETS1 Service Provider Alert	Mandatory SMETS1	RSA

8.1.25. DCC Alert Tests - OU

Reference	Name	Test Scenario	Applicable User Role
N24	Update HAN Device Log Result - Successful Communications Hub Function Whitelist Update	Mandatory SMETS2+	OU
N55	SMETS1 Service Provider Alert	Mandatory SMETS1	OU

8.1.26. Response Code Tests

The following table outlines the Response Code Tests required to be executed by User Role. The purpose of these tests is to prove that a party can receive a subset of Response Code messages based on the differing types of response codes that can be received.

New User

The following User Role tables reflect the test Response Codes that must be executed by a new Party seeking to undertake UEPT, unless the Testing Participant has descoped a subset of Service Requests and this have been agreed with DCC or, where referred to the Panel, has been determined by the Panel. The tests are those indicated as 'Mandatory, Mandatory SMETS1 and Mandatory SMETS2+ ' in the test scenario column, for which they must be executed for each specific User Role. Those indicated as 'Mandatory' must be executed in respect of a SMETS1 Device and a SMETS2+ Device. Those indicated as 'Mandatory SMETS1' must be executed in respect of a SMETS1 Device. Those indicated as 'Mandatory SMETS2+' must be executed in respect of a SMETS2+ Device. Where the Response Code Tests are indicated as N/A there is no requirement to test during execution of the test scenarios.

Reference	Name	Test Scenario	User Role
E11	Failed Validation - Invalid Service Request / Device Type combination	Mandatory	IS ES GS ED GT RSA MDR OU
E13	Failed Validation – Invalid Request Type for URL	Mandatory	IS ES GS ED GT RSA MDR OU
E19	Failed Validation – Device doesn't exist	Mandatory	IS ES GS ED GT RSA MDR OU
E60	Failed Validation – Invalid Service Request for SMETS1 Devices	Mandatory SMETS1	IS ES GS ED GT RSA MDR OU
E61	Failed Validation – Invalid Command Variant for SMETS1 Service Request	Mandatory SMETS1	IS ES GS ED GT RSA MDR OU

8.1.27. Self Service Interface Test

The following tables outline the test required to be executed by a Testing Participant to determine whether the prospective User can access the SSI.

	Test Scenario
Title:	Testing Participant can successfully log into and access the Self Service Interface.
Prerequisite:	• Testing Participant holds the role of IS, IS, ES, ED, GT, RSA, MDR or OU for testing purposes. • Connection to DCC System. • Party SSI login authentication via DCC or own IDP.

Steps	Description	Objective	Actions	Acceptance Criteria
1	Login via IDP	Authenticate via IDP	Party to open the web service for SSI logon and complete Party login via DCC or own IDP.	Login success and the authenticating SEC Party will be presented with Self Service Interface.

9. Annex D: Forms and Templates

Extant versions of templates for the following documents will be maintained on the DCC Website or SharePoint.

Forms and Templates
Party Notification of Intention to Undertake Testing Template
DCC Acknowledgement of Intention to Undertake Testing template
Test Readiness Report template
Test Plan template
Test Execution Dashboard template
Test Completion Report template

10. Annex E: UEPT AND ADDITIONAL SR TEST COMPLETION CERTIFICATE

UEPT AND ADDITIONAL SR TEST COMPLETION CERTIFICATE

To:[Party]

From:[DCC]

[Date]

Dear Sir or Madam,

TEST COMPLETION CERTIFICATE UEPT OR ADDITIONAL SR TESTING

We confirm that the relevant Exit Criteria have been achieved in respect of UEPT or Additional SR Testing

Party: [Party]

SEC Party Signifier: [Signifier]

User Role: [User Role]

The table, below, includes all SRs the Party has completed either UEPT or Additional SR Testing to date as indicated by the Date Test Completion Certificate issued column.

Service Request Variant	Tested as part of UEPT or Additional SR Testing	Date Test Completion Certificate issued

Yours faithfully

[Name]

[Position]

Acting on behalf of the DCC

11. Annex F: DEFINITIONS

Term	Definition	Source
Entry Criteria	The criteria that must be satisfied before testing can commence	Clause 5.8 of this document
Exit Criteria	The criteria that must be satisfied before testing can be considered complete	Clause 5.19 of this document
SMETS2+ Install and Commission	The process of installing and commissioning a SMEST2+ Communications Hub Function, a SMETS+ Gas Proxy Function (in the case of Gas Smart Meters) and SMETS2+ Smart Meters with the DCC.	Clause 5.1 of this document
Regression Testing	Testing of a previously tested programme following modification of that programme to ensure that defects have not been introduced or uncovered in unchanged areas of the software, as a result of the changes made (and Regression Test shall be construed accordingly)	International Software Testing Qualifications Board
Relevant Party	The Party which is undertaking the necessary steps for the purposes of User Entry Process Tests	This document
(Requirements) Traceability Matrix	A matrix of defined requirements that provides traceability (linkage) to Test Scripts for the purpose of providing a measurement of test coverage.	International Software Testing Qualifications Board
Test Completion Certificate	A certificate issued by the DCC to a Party in a particular User Role upon request and in any event in accordance with 5.6.1.3 when that Party successfully completes UEPT.	Clause 10 of this document
Test Completion Report	A document summarising testing activities and results. It also contains an evaluation against Exit Criteria.	Clause 6.6 of this document
Test Data	The data constructed for the purposes of undertaking User Entry Process Tests	Clause 7 of this document
Test Data Plan	The document that sets out: the size and type/format of data, who is responsible for providing the data; and when the data is required to be available to support test activities in a Test Plan	Clause 7 of this document
Test Execution Dashboard	The document summarising testing activities and results, produced at regular intervals, to report progress of testing activities against a baseline (such as the original test plan) and to communicate risks.	Clause 6.5 of this document

Test Management Tool	A tool that has the ability to log and track Testing Issues.	Clause 5.19.1 of this document
Test Plan	A document describing the scope, approach, resources and schedule of intended test activities within a Test Stage that will be produced as set out in clause 6.1.4	Clause 6.4 of this document
Test Result	The consequence/outcome of the execution of a test script	Clause 6.4 of this document
Test Readiness Report	A report that when completed provides the capability to assess the status of test preparation and determine the readiness to proceed into test execution	Clause 6.3 of this document
Test Schedule	A list of test process activities, tasks or events identifying their intended start and finish dates and/or times and interdependencies.	Clause 6.4 of this document
Test Script	A document specifying a sequence of actions for the execution of a test	Clause 6.8 of this document

References

Abbreviation	**Title & Originator's Reference**
SEC	Smart Energy Code
DUIS	DCC User Interface Specification
ETAD	Enduring Testing Approach Document
E2EAD	End to End Testing Approach Document
None	Guide for Testing Participants

12. Annex G: Testing Issue Severity Descriptions

Severity	Description
Severity 1	An Issue which in relation to the Relevant Party: • would prevent user from using their systems • would have a critical adverse impact on business activities • would cause significant financial loss • would result in any material loss or corruption of Data. Non-exhaustive examples: • an Issue leading to non-availability of systems • all test progress is blocked.
Severity 2	An Issue which in relation to the Relevant Party: • would have a major (but not critical) adverse impact on use of systems • would cause limited financial loss Non-exhaustive examples: • an Issue leading to non-availability of or to loss of resilience of a material part of their systems • large areas of functionality will not be able to be tested • testing not completely blocked but has been significantly impacted.
Severity 3	An Issue which in relation to the Relevant Party: • would have a major adverse impact on business activities but which can be reduced to a moderate adverse impact through a work-around • would have a moderate adverse impact on the business activities Non-exhaustive examples: • testing can progress but the work-around will impact test progress.
Severity 4	An Issue which in relation to the Relevant Party: • would have a minor adverse impact on business activities Non-exhaustive examples: • minor service interruptions in the business process
Severity 5	An Issue which in relation to the Relevant Party: • would have minimal impact on business activities Non-exhaustive examples: • trivial Issues with work-arounds which are noted for future releases but minimal impact of running existing activities • tests can still pass but there are cosmetic issues.

Version: 7.0

Appendix S

DCCKI Certificate Policy

Contents

1 INTRODUCTION

(a) The document (together with its Annexes A and B):

(i) shall be known as the "DCCKI Certificate Policy" (and in this document is referred to simply as the "Policy"); and

(ii) is a SEC Subsidiary Document related to Section L13.34(a)(i) (The DCCKI SEC Documents) of the Code.

1.1 Overview

(a) This Policy sets out the arrangements relating to:

(i) The Root DCCKICA Certificate;

(ii) EII DCCKICA Certificates; and

(iii) UI DCCKICA Certificates;

together referred to as the "**DCCKICA Certificates"** and

(iv) DCCKI Infrastructure Certificates; and

(v) Personnel Authentication Certificates,

together with the DCCKICA Certificates referred to as the "**DCCKI Certificates**".

(b) This Policy is structured according to the guidelines provided by IETF RFC 3647, with appropriate extensions, modifications and deletions.

1.2 Document Name and Identification

(a) This Policy has been registered with the Internet Address Naming Authority and assigned an OID of 1.2.826.0.1.8641679.1.2.1.11.

1.3 DCCKI Participants

1.3.1 The DCCKI Certification Authority

(a) The definition of the DCCKI Certification Authority is set out in Annex A.

1.3.2 DCCKI Registration Authority

(a) The definition of the DCCKI Registration Authority is set out in Annex A.

1.3.3 DCCKI Subscribers

(a) In accordance with Section L13.2 of the Code (DCCKI Authorised Subscribers) Parties and Registration Data Providers (RDPs) may become DCCKI Authorised Subscribers.

(b) The DCCKI RAPP section 3 sets out the procedure to be followed by Parties and RDPs in order to become a DCCKI Authorised Subscriber for one or more DCCKI Certificates.

(c) The DCC (acting in its capacity as the Root DCCKICA, EII DCCKICA or UI DCCKICA) shall be a DCCKI Authorised Subscriber and:

(i) it (and only it) shall be a DCCKI Eligible Subscriber in respect of DCCKICA Certificates; and

(ii) (save for the purpose of replacement of the Root DCCKICA), it shall be a DCCKI Eligible Subscriber only in respect of a single Root DCCKICA Certificate.

(d) Where a person is a DCCKI Authorised Subscriber in accordance with this Policy and the DCCKI RAPP, that person shall be a DCCKI Eligible Subscriber in respect of DCCKI Infrastructure Certificates where the purpose of that DCCKI Certificate is:

(i) establishing TLS communications with the DCC over a DCC Gateway Connection, and that person is a Party or RDP; or

(ii) the signing of SAML assertions in order to Authenticate its User Personnel to the Self Service Interface using an Identity Provider Service that is not the DCC Identity Provider Service, and that person is a User.

(e) A Party that is a DCCKI Authorised Subscriber shall be a DCCKI Eligible Subscriber in respect of Personnel Authentication Certificates only in the circumstance where that DCCKI Authorised Subscriber is a User, intending to use the Identity Provider Service provided by the DCC for the purpose of Authenticating its User Personnel to the Self Service Interface as set out in Part 1.4.1 of this Policy.

(f) DCCKI Eligible Subscribers and DCCKI Subscribers are subject to the applicable requirements of this Policy, the DCCKI RAPP and Sections L13.43 to L13.47 (The DCCKI Subscriber Obligations) of the Code.

(g) The definitions of the following terms are set out in Section A of the Code (Definitions and Interpretations):

(i) DCCKI Subscriber; and

(ii) DCCKI Eligible Subscriber.

(h) The definition of a DCCKI Authorised Subscriber is set out in Annex A to this Policy.

1.3.4 DCCKI Relying Parties

(a) The definition of a DCCKI Relying Party is set out in Section A of the Code (Definitions and Interpretations).

(b) DCCKI Relying Parties shall be subject to the applicable requirements of Sections L13.48 to L13.52 (The DCCKI Relying Party Obligations) of the Code.

1.3.5 DCCKI Policy Management Authority

(a) The DCC shall fulfil the functions of the DCCKI PMA in accordance with the provisions set out in Sections L13.53 to L13.57 (The DCCKI PMA Functions) of the Code.

1.3.6 DCCKI Repository Provider

(a) Provision in relation to the DCCKI Repository Service is made in Section L13.18 (The DCCKI Repository Service) of the Code.

1.4 USAGE OF DCCKI CERTIFICATES

1.4.1 Appropriate Certificate Uses

(a) The DCCKICA shall ensure that DCCKICA Certificates are Issued only to:

(i) the Root DCCKICA for use in its capacity as, and for the purposes of, exercising its functions as the Root DCCKICA; and

(ii) the EII DCCKICA and the UI DCCKICA, in their capacity as, and for the purposes of exercising the functions of, issuing authorities.

(b) Subject to 1.4.1 (e), the DCCKICA shall ensure that DCCKI Infrastructure Certificates are Issued only:

(i) by the EII DCCKICA, and to DCCKI Eligible Subscribers; and

(ii) for the purposes of:

(1) establishing TLS communications with the DCC over a DCC Gateway Connection; or

(2) the signing of SAML assertions of a User that chooses to Authenticate its User Personnel to the Self Service Interface using an Identity Provider Service that is not provided by the DCC; or

(3) supporting the Transfer of Secret Key Material as defined in Section G2.22F to G2.22I.

(c) Subject to 1.4.1 (e), the DCCKICA shall ensure that Personnel Authentication Certificates are Issued only:

(i) by the UI DCCKICA, and to DCCKI Eligible Subscribers; and

(ii) for the purpose of Authenticating User Personnel of Users intending to use the Identity Provider Service provided by the DCC to the Self Service Interface.

(d) Further provision in relation to Parties and RDPs obligations in respect of the use of DCCKI Certificates is made in Sections L13.43 to L13.47 (The DCCKI Subscriber Obligations) of the Code and Sections L13.48 to L13.52 (The DCCKI Relying Party Obligations) of the Code.

(e) Nothing in this DCCKI Certificate Policy shall prevent DCC from:

(i) using the Root DCCKICA Certificate for the purposes of issuing additional issuing authority certificates;

(ii) using those issuing authorities to issue additional end entity certificates; or

(iii) issuing DCCKI Infrastructure Certificates or Personnel Authentication Certificates to DCC or DCC Service Providers other than in accordance with this Policy;

provided that in any of the above cases DCC may only do so:

(iv) for the purposes of issuing DCCKI Certificates or other certificates as may be required to establish secure communications between DCC and DCC Service Providers, or to secure communications and data within DCC Service Providers, but not between either DCC or a DCC Service Provider and any other Party or RDP;

(v) to the extent set out in the DCCKI Certification Practice Statement; and

(vi) other than in the cases specified in 1.4.1(a) to (c) above, subject to SMKI PMA approval.

1.4.2 Prohibited Certificate Uses

(a) No Party or Registration Data Provider shall use a DCCKI Certificate other than for the purposes permitted in Part 1.4.1 of this Policy.

1.5 Policy Administration

1.5.1 Organisation Administering the Document

(a) This Policy is a SEC Subsidiary Document and shall be maintained in accordance with the provisions of the Code.

1.5.2 Contact Person

(a) Questions in relation to the content of this Policy should be addressed to the DCCKI PMA or the Service Desk.

1.5.3 Person determining Certification Practice Statement suitability for the Policy

(a) Provision is made in Section L13.38 (the DCCKI Certification Practice Statement) of the Code in relation to the suitability of the DCCKI CPS for the Policy.

1.5.4 CPS Approval Procedures

(a) Provision is made in Section L13.54 (the DCCKI PMA Functions) of the Code for the procedure by which the DCCKI PMA may approve the DCCKI CPS.

1.5.5 Registration Authority Policies and Procedures

(a) The DCCKI Registration Authority Policies and Procedures are set out at Appendix W of the Code.

2 PUBLICATION AND REPOSITORY RESPONSIBILITIES

2.1 Repositories

(a) Provision is made in Section L13.18 (the DCCKI Repository Service) of the Code for the establishment, operation and maintenance of the DCCKI Repository.

2.2 Publication of Certification Information

(a) Section L13.19 (the DCCKI Repository Service) of the Code makes provision for the lodging of documents and information in the DCCKI Repository.

2.3 Time or Frequency of Publication

(a) The DCCKICA shall ensure that:

(i) Root DCCKICA Certificate and EII DCCKICA Certificate are lodged promptly in the DCCKI Repository on Issuance;

(ii) each new version of the EII DCCKICA Certificate Revocation List is lodged in the DCCKI Repository following its production as is specified in Part 4.9.7 of this Policy;

(iii) each new version of the DCCKI Authority Revocation List is lodged in the DCCKI Repository following its production as is specified in Part 4.9.7 of this Policy;

(iv) DCCKI Infrastructure Certificates are lodged promptly in the DCCKI Repository on Issuance; and

(v) a revised version of the DCCKI RAPP is lodged promptly in the DCCKI Repository following each modification.

2.4 Access Control on Repositories

(a) Provision in relation to access controls for the DCCKI Repository is made in Section L13.21 (the DCCKI Repository Service) of the Code and the DCCKI Interface Design Specification and the DCCKI Certification Practice Statement.

3 IDENTIFICATION AND AUTHENTICATION

3.1 Naming

3.1.1 Types of Names

(a) Provision is made in the DCCKI RAPP section 5.1 to ensure that the name of the Subject of each DCCKI Certificate is in accordance with the relevant DCCKI Certificate Profile in Annex B to this document.

3.1.2 Need for Names to be Meaningful

(a) Provision is made in the DCCKI RAPP section 5.1 to ensure that the name of the Subject of each DCCKI Infrastructure Certificate is meaningful and consistent with the relevant DCCKI Certificate Profile in Annex B to this document.

3.1.3 Anonymity or Pseudonymity of Subscribers

(a) Provision is made in the DCCKI RAPP section 5.5 to prohibit DCCKI Eligible Subscribers from requesting the Issue of a DCCKI Certificate anonymously or by means of a pseudonym.

3.1.4 Rules for Interpreting Various Name Forms

(a) Provision in relation to name forms is made in Annex B to this document.

3.1.5 Uniqueness of Names

(a) Provision in relation to the uniqueness of names is made in Annex B to this document.

3.1.6 Recognition, Authentication, and Role of Trademarks

(a) Provision in relation to the use of trademarks, trade names and other restricted information in DCCKI Certificates is made in Section L13.44 (DCCKI Certificate Signing Requests and Personnel Authentication Certificate Applications) of the Code.

3.2 Initial Identity Validation

3.2.1 Method to Prove Possession of Private Key

(a) Provision is made in the DCCKI RAPP section 5.6 in relation to:

(i) the procedure to be followed by a DCCKI Eligible Subscriber in order to prove its possession of the Private Key that is associated with the Public Key to be contained in any DCCKI Infrastructure Certificate that is the subject of a DCCKI Certificate Signing Request which has been submitted by that Eligible Subscriber; and

(ii) that the procedure established for this purpose is in accordance with the procedure in PKCS#10 or an equivalent cryptographic mechanism as agreed by the DCCKI PMA function.

(b) Provision is made in the DCCKI CPS in relation to:

(i) the procedure to be followed by the DCCKICA in order to prove its possession of the Private Key that is associated with the Public Key to be contained in any DCCKICA Certificate that is the subject of a DCCKI Certificate Signing Request; and

(ii) the procedure to be followed by the DCCKICA in order to prove its possession of the Private Key that is associated with the Public Key to be contained in any Personnel Authentication Certificate that is the subject of a DCCKI Certificate Signing Request pursuant to a Personnel Authentication Certificate Application from an Eligible Subscriber.

3.2.2 Authentication of Organisation Identity

(a) Provision is made in the DCCKI RAPP section 3 in relation to:

(i) The procedure to be followed by a Party or RDP in order to become a DCCKI Authorised Subscriber;

(ii) The criteria in accordance with which the DCCKI Registration Authority shall determine whether a Party or RDP is entitled to become a DCCKI Authorised Subscriber;

(iii) The requirement that the Party or RDP shall be Authenticated by the DCCKICA for that purpose; and

(iv) The criteria in accordance with which the DCCKICA shall determine whether a Party or RDP is Authenticated.

3.2.3 Authentication of Individual Identity

(a) Provision is made in the DCCKI RAPP in relation to the Authentication of individuals engaged by DCCKI Authorised Subscribers to fulfil roles defined in this Policy.

3.2.4 Non-verified Subscriber Information

(a) The DCCKICA shall verify all information in relation to DCCKI Certificates, save that the Subject name for Personnel Authentication Certificates is derived from the information input by DCCKI Eligible Subscriber for the purposes of populating fields in those Personnel Authentication Certificates and need not be verified by the DCCKICA.

3.2.5 Validation of Authority

See Part 3.2.2 of this Policy.

3.2.6 Criteria for Interoperation

[Not applicable]

3.3 Identification and Authentication for re-key Requests

3.3.1 Identification and Authentication for Routine Re-Key

(a) This Policy does not support Certificate Re-Key.

(b) The DCCKICA shall not provide a Certificate Re-Key service.

3.3.2 Identification and Authentication for Re-Key after Revocation

[Not applicable]

3.4 Identification and Authentication for Revocation Requests

3.4.1 Authentication for Certificate Revocation Requests

(a) Provision is made in the DCCKI RAPP section 6.10 in relation to procedures designed to ensure the Authentication of persons who submit a DCCKI Certificate Revocation Request and to verify that they are authorised to submit that request.

4 CERTIFICATE LIFE-CYCLE OPERATIONAL REQUIREMENTS

4.1 Certificate Applications

4.1.1 Submission of Certificate Applications

(a) Provision is made in the DCCKI RAPP section 5 with respect to the circumstances in which an DCCKI Eligible Subscriber may:

(i) submit a DCCKI Certificate Signing Request in relation to a DCCKI Infrastructure Certificate;

(ii) submit a Personnel Authentication Certificate Application in relation to a Personnel Authentication Certificate; and

(iii) submit a DCCKI Certificate Signing Request in relation to a DCCKICA Certificate,

and, in each case, the means by which that DCCKI Eligible Subscriber may do so.

4.1.2 Enrolment Process for the Subscriber and its Representatives

(a) Provision is made in the DCCKI RAPP section 3 in relation to the:

(i) establishment of an enrolment process in relation to Parties and RDPs in order to Authenticate them and verify that they are authorised to act as DCCKI Authorised Subscribers;

(ii) establishment of an enrolment process in relation to individuals nominated to act on behalf of DCCKI Authorised Subscribers as DCCKI Senior Responsible Officers or DCCKI Authorised Responsible Officers, in order to Authenticate them and verify that they are authorised to act on behalf of (and, in the case of Personnel Authentication Certificate Applications, go on to authorise others to act on behalf of) those DCCKI Authorised Subscribers; and

(iii) maintenance by the DCCKICA of a list of Parties, RDPs, and individuals enrolled in accordance with those enrolment processes.

4.1.3 Enrolment Process for the Registration Authority and its Representatives

(a) Provision is made in the DCCKI RAPP section 4 in relation to the establishment of an enrolment process in respect of DCCKICA Personnel and DCCKICA Systems for the purpose of Authentication and to verify that they are authorised to act on behalf of the DCCKICA in its capacity as the DCCKI Registration Authority; including in particular, for that purpose, provision for:

(i) the Authentication of all DCCKI Registration Authority Personnel by a DCCKI Registration Authority Manager; and

(ii) all DCCKI Registration Authority Personnel to have their identity and authorisation verified prior to being provided these roles.

4.2 Certificate Application Processing

4.2.1 Performing Identification and Authentication Functions

(a) Provision is made in the DCCKI RAPP in relation to the Authentication by the DCCKICA of a DCCKI Eligible Subscriber which submits:

(i) a DCCKI Certificate Signing Request in relation to a DCCKI Infrastructure Certificate; or

(ii) a Personnel Authentication Certificate Application in relation to a Personnel Authentication Certificate.

4.2.2 Approval or Rejection of Certificate Applications

(a) Where any DCCKI Certificate Signing Request made in relation to a DCCKI Infrastructure Certificate fails to satisfy the requirements set out in the DCCKI RAPP, this Policy or any other provisions of the Code, the DCCKICA:

(i) shall reject it and refuse to Issue the DCCKI Infrastructure Certificate which was the subject of that DCCKI Certificate Signing Request, and

(ii) shall give notice to the person that made the DCCKI Certificate Signing Request of the reasons for its rejection.

(b) Where the failure results from a failure of Authentication of the DCCKI Eligible Subscriber, then an Incident shall be raised by DCCKICA Personnel.

(c) Where any DCCKI Certificate Signing Request satisfies the requirements set out in the DCCKI RAPP, this Policy, and any other provision of the Code, the DCCKICA shall Issue the DCCKI Certificate that was the subject of that DCCKI Certificate Signing Request.

4.2.3 Time to Process Certificate Applications

(a) Provision is made in the DCCKI RAPP in relation to the agreed elapsed time for the processing of DCCKI Certificate Signing Requests and Personnel Authentication Certificate Applications made in accordance with this Policy.

4.3 DCCKI Certificate Issuance

4.3.1 DCCKICA actions during certificate Issuance

(a) The Root DCCKICA shall Issue a DCCKICA Certificate only in accordance with the provisions of this Policy and the DCCKI CPS.

(b) The DCCKICA shall Issue a DCCKI Infrastructure Certificate or a Personnel Authentication Certificate only in accordance with the provisions of this Policy and the DCCKI RAPP and:

(i) in the case of DCCKI Infrastructure Certificates, only in response to a DCCKI Certificate Signing Request made by a DCCKI Eligible Subscriber; and

(ii) in the case of Personnel Authentication Certificates, only following the creation of a DCCKI Certificate Signing Request by the DCCKICA in response to a Personnel Authentication

Certificate Application made by a member of User Personnel of a DCCKI Eligible Subscriber via the Personnel Credentials Interface.

(c) The DCCKICA shall ensure that each DCCKI Certificate that is Issued by it contains information that:

(i) it has verified to be correct and complete; and

(ii) is consistent with the information in the DCCKI Certificate Signing Request.

4.3.2 Notification to DCCKI Eligible Subscriber by the DCCKICA of Issuance of Certificate

(a) Provision is made in the DCCKI RAPP for the DCCKICA to notify a DCCKI Eligible Subscriber of the Issuance of a DCCKI Certificate which was the subject of a DCCKI Certificate Signing Request or Personnel Authentication Certificate Application made by it.

4.4 Certificate Acceptance

4.4.1 Conduct Constituting Certificate Acceptance

(a) Provision is made in the DCCKI RAPP to:

(i) specify the means by which an DCCKI Eligible Subscriber may clearly indicate to the DCCKICA its rejection of a DCCKI Certificate which has been Issued to it; and

(ii) specify the circumstances in which a DCCKI Eligible Subscriber is treated as a DCCKI Subscriber in relation to a DCCKI Certificate.

(b) Further provision in relation to subscribing for or rejecting DCCKI Certificates is made in Section L13.45 (Subscribing for or Rejecting DCCKI Certificates) of the Code.

4.4.2 Publication of Certificates by the DCCKICA

(a) Following Issuance, the DCCKICA shall lodge a copy of each Root DCCKICA Certificate, each EII DCCKICA Certificate and each DCCKI Infrastructure Certificate in the DCCKI Repository.

(b) Further provision in relation to the publication of DCCKI Certificates is made in Part 2 of this Policy and in Section L13.17 (the DCCKI Repository Service) of the Code.

4.4.3 Notification of Certificate Issuance by the DCCKICA to Other Entities

(a) The DCCKICA shall give explicit notice of the Issue of a DCCKI Certificate only to the DCCKI Eligible Subscriber who submitted the DCCKI Certificate Signing Request or Personnel Authentication Certificate Application.

4.5 Key Pair and Certificate Usage

4.5.1 DCCKI Authorised Subscriber Private Key and Certificate Usage

(a) Provision for restrictions on the use by DCCKI Authorised Subscribers of Private Keys in respect of DCCKI Certificates is made in:

(i) Section G5.24 (the User Information Security Management System) of the Code;

(ii) Section L13 (DCC Key Infrastructure) of the Code;

(iii) this Policy; and

(iv) the DCCKI Certification Practice Statement.

4.5.2 DCCKI Relying Party Public Key and Certificate Usage

(a) Provision in relation to reliance that may be placed on a DCCKI Certificate is made in Section L13.48 to L13.52 (the DCCKI Relying Party Obligations) of the Code.

4.6 Certificate Renewal

4.6.1 Circumstances of Certificate Renewal

(a) This Policy does not support the renewal of DCCKI Certificates.

(b) The DCCKICA may only replace, and shall not renew, any DCCKI Certificate.

4.6.2 Circumstances of Certificate Replacement

(a) A DCCKI Certificate replacement may occur:

(i) where the request for DCCKI Certificate replacement relates to normal business activity, in which case the process set out in the DCCKI RAPP shall apply;

(ii) where suspicion of Compromise or Compromise is reported for a DCCKI Certificate that has been issued; in which case the matter shall be managed through the Incident Management Policy and in accordance with the DCCKI RAPP.

4.6.3 Who May Request a Replacement Certificate

See Part 4.1 of this Policy.

4.6.4 Processing Replacement Certificate Requests

See Part 4.2 of this Policy.

4.6.5 Notification of Replacement Certificate Issuance to a Subscriber

See Part 4.3 of this Policy.

4.6.6 Conduct Constituting Acceptance of a Replacement Certificate

See Part 4.4 of this Policy.

4.6.7 Publication of a Replacement Certificate by the DCCKICA

See Part 4.4.2 of this Policy.

4.6.8 Notification of Certificate Issuance by the DCCKICA to Other Entities

See Part 4.4.3 of this Policy.

4.7 Certificate Re-Key

(a) This Policy does not support Certificate Re-Key.

4.7.1 Circumstances for Certificate Re-Key

[Not applicable]

4.7.2 Who may request Certificate re-key

[Not applicable]

4.7.3 Processing Certificate Re-Keying Requests

[Not applicable]

4.7.4 Notification of New Certificate Issuance to Subscriber

[Not applicable]

4.7.5 Conduct Constituting Acceptance of a Re-Keyed Certificate

[Not applicable]

4.7.6 Publication of the Re-Keyed Certificate by the DCCKICA

[Not applicable]

4.7.7 Notification of Certificate Issuance by the DCCKICA to Other Entities

[Not applicable]

4.8 Certificate Modification

(a) This Policy does not support DCCKI Certificate modification.

4.8.1 Circumstances for Certificate Modification

[Not applicable]

4.8.2 Who may request Certificate Modification

[Not applicable]

4.8.3 Processing Certificate Modification Requests

[Not applicable]

4.8.4 Notification of New Certificate Issuance to Subscriber

[Not applicable]

4.8.5 Conduct Constituting Acceptance of Modified Certificate

[Not applicable]

4.8.6 Publication of the Modified Certificate by the DCCKICA

[Not applicable]

4.8.7 Notification of Certificate Issuance by the DCCKICA to Other Entities

[Not applicable]

4.9 Certificate Revocation and Suspension

4.9.1 Circumstances for Revocation

(a) In accordance with the DCCKI RAPP, the DCCKICA may revoke DCCKI Certificates that have been Issued to a DCCKI Subscriber:

(i) at that DCCKI Subscriber's request, as described in the DCCKI RAPP;

(ii) in accordance with Incident Management processes or, in the event of a Major Security Incident, where DCC reasonably believes that Compromise of that DCCKI Subscriber's Private Key has occurred;

(iii) (subject to the Section L16.1 (Supplier of Last Resort) of the Code) where an organisation ceases to be a DCCKI Eligible Subscriber in relation to that DCCKI Certificate;

(iv) in the circumstances described in Section H10.1 (Emergency Suspension of Services) of the Code; and

(v) (subject to the Section L16.1 (Supplier of Last Resort) of the Code) where a request is received by DCC from the Panel in the circumstances set out in Section M8 (Suspension, Expulsion, and Withdrawal) of the Code that would result in a requirement to revoke one or more DCCKI Certificates that have been Issued to that DCCKI Subscriber.

4.9.2 Who can Request Revocation

(a) In accordance with the DCCKI RAPP and Part 4.9.1 of this Policy, the following may request the revocation of DCCKI Certificates:

(i) a DCCKI Authorised Subscriber in relation to DCCKI Infrastructure Certificates for which it is a DCCKI Subscriber; and

(ii) the DCC.

4.9.3 Procedure for Revocation Request

(a) Provision is made in the DCCKI RAPP in relation to the procedure for submitting and processing a DCCKI Certificate Revocation Request.

4.9.4 Revocation Request Grace Period

(a) Provision is made in the DCCKI RAPP in relation to the grace period for requesting a DCCKI Certificate revocation.

4.9.5 Time within which the DCCKICA must process the Revocation Request

(a) The DCCKICA shall ensure that it processes all DCCKI Certificate Revocation Requests as soon as reasonably practicable following receipt and in accordance with the procedures set out in the DCCKI RAPP.

4.9.6 Revocation Checking Requirements for Relying Parties

(a) Provision in relation to the revocation checking requirements for DCCKI Relying Parties is made in Section L13 (DCC Key Infrastructure) of the Code.

4.9.7 CRL Issuance Frequency

(a) The DCCKICA shall ensure that an up to date version of any DCCKI ARL is lodged in the DCCKI Repository:

(i) at least once in every period of twelve months; and

(ii) promptly on the revocation of a EII DCCKICA Certificate or UI DCCKICA Certificate.

(b) Each version of the DCCKI ARL shall be valid until the date which is up to 13 months after the date on which that version is lodged in the DCCKI Repository or until it is subsequently replaced with an updated version.

(c) The DCCKICA shall ensure that each up to date version of the DCCKI ARL:

(i) continues to include each relevant revoked EII DCCKICA Certificate and relevant revoked UI DCCKICA Certificate until such time as the Validity Period of that EII DCCKICA Certificate or UI DCCKICA Certificate has expired; and

(ii) does not include any revoked EII DCCKICA Certificate or revoked UI DCCKICA Certificate after the Validity Period of that EII DCCKICA Certificate or UI DCCKICA Certificate has expired.

(d) The EII DCCKICA shall ensure that an up to date version of the EII DCCKICA CRL is lodged in the DCCKI Repository:

(i) at least once in every period of 30 days; and

(ii) within one hour on the revocation of a DCCKI Infrastructure Certificate.

(e) The EII DCCKICA shall ensure that each up to date version of the EII DCCKICA CRL:

(i) continues to include each relevant revoked DCCKI Infrastructure Certificate until such time as the Validity Period of that DCCKI Infrastructure Certificate has expired; and

(ii) does not include any revoked DCCKI Infrastructure Certificate after the Validity Period of that DCCKI Infrastructure Certificate has expired.

(f) The EII DCCKICA shall ensure that the EII DCCKICA CRL contains a non-critical entry extension which identifies the reason for the revocation of each DCCKI Infrastructure Certificate listed on it in accordance with RFC 5280 or an equivalent cryptographic standard.

(g) The UI DCCKICA shall not lodge a version of the UI DCCKICA CRL in the repository.

4.9.8 Maximum Latency for DCCKI CRLs (if applicable)

(a) In accordance with Part 4.9.7.

4.9.9 On-line Revocation/Status Checking Availability

[Not applicable]

4.9.10 On-line Revocation Checking Requirements

[Not applicable]

4.9.11 Other Forms of Revocation Advertisements Available

[Not applicable]

4.9.12 Special Requirements in the Event of Key Compromise

(a) See Part 4.6.2 of this Policy.

4.9.13 Circumstances for Suspension

(a) This Policy does not support suspension of DCCKI Certificates.

4.9.14 Who can Request Suspension

[Not Applicable]

4.9.15 Procedure for Suspension Request

[Not Applicable]

4.9.16 Limits on Suspension Period

[Not Applicable]

4.10 Certificate Status Services

4.10.1 Operational Characteristics

[Not applicable]

4.10.2 Service Availability

[Not applicable]

4.10.3 Optional Features

[Not applicable]

4.11 End of Subscription

(a) Provision is made in the DCCKI RAPP in relation to end of subscription.

4.12 KEY ESCROW AND RECOVERY

(a) This Policy does not support Key Escrow.

(b) The DCCKICA shall not provide a Key Escrow service.

4.12.1 Key Escrow and Recovery Policies and Practices

[Not applicable]

4.12.2 Session Key Encapsulation and Recovery Policy and Practices

[Not applicable]

5 FACILITY, MANAGEMENT, AND OPERATIONAL CONTROLS

5.1 Physical Controls

5.1.1 Site location and construction

(a) The DCCKICA shall ensure that the DCCKICA Systems are operated in a sufficiently secure environment which shall at least satisfy the requirements set out in Section G2 (System Security: Obligations on the DCC) and Section G5 (Information Security: Obligations on the DCC and Users) of the Code.

(b) The DCCKICA shall ensure that the DCCKI CPS incorporates provisions in relation to physical controls including in particular provisions designed to ensure that:

(i) all of the physical locations in which the DCCKICA Systems are situated, operated, routed or directly accessed are in the United Kingdom;

(ii) all bespoke Security Related Functionality is developed, specified, designed, built and tested only within the United Kingdom;

(iii) all Security Related Functionality is integrated, configured, tested in situ, implemented, operated and maintained only within the United Kingdom;

(iv) the DCCKICA Systems cannot be indirectly accessed from any location outside the United Kingdom;

(v) the Root DCCKICA shall operate as a secure offline entity that is Separate from the rest of the DCC Systems; and

(vi) all Private Keys used to support the DCCKICA are generated, stored and processed within the cryptographic envelope of a Cryptographic Module which meets the FIPS 140-2 Level 3or equivalent cryptographic standard.

(c) The functions of the DCCKI Registration Authority shall securely interoperate with the other operational elements of the DCCKICA, as detailed in the DCCKI CPS.

5.1.2 Physical access

(a) The DCCKICA shall ensure that the DCCKI CPS incorporates provisions in relation to access control including in particular provisions designed to:

(i) establish and maintain controls such that only appropriately authorised personnel may have unescorted physical access to DCCKICA Systems;

(ii) ensure that any unauthorised personnel may have physical access to DCCKICA Systems only if appropriately authorised and supervised;

(iii) ensure that site access procedures are audited as part of both internal audits and third party audits carried out in accordance with ISO/IEC 27001;

(iv) ensure that all material in relation to cryptographic operation is securely managed; and

(v) ensure that removable media which contain sensitive data are kept in secure locations, managed through life and disposal and, accessible only to appropriately authorised individuals.

5.1.3 Power and air conditioning

(a) The DCCKICA shall ensure that the DCCKI CPS incorporates provisions in relation to power and air conditioning at all physical locations in which the DCCKICA Systems are situated.

5.1.4 Water exposure

(a) The DCCKICA shall ensure that the DCCKI CPS incorporates provisions in relation to water exposure at all physical locations in which the DCCKICA Systems are situated.

5.1.5 Fire prevention and protection

(a) The DCCKICA shall ensure that the DCCKI CPS incorporates provisions in relation to fire prevention and protection at all physical locations in which the DCCKICA Systems are situated.

5.1.6 Media storage

(a) The DCCKICA shall ensure that the DCCKI CPS incorporates provisions in relation to media storage at all physical locations in which the DCCKICA Systems are situated.

5.1.7 Waste disposal

(a) The DCCKICA shall ensure that all media used to store Data held by it for the purposes of carrying out its functions is securely disposed of in accordance with https://www.ncsc.gov.uk/guidance/secure-sanitisation-storage-media.

5.1.8 Off-site backup

(a) The DCCKICA shall ensure that the DCCKI CPS incorporates provisions in relation to off-site back up and data management of data held in the DCCKICA Systems.

(b) The DCCKICA shall ensure that backups shall be made to support disaster recovery models as defined within the DCCKI CPS.

(c) The DCCKICA shall ensure that:

(i) regular backups of critical DCCKICA and DCCKI Registration Authority operational data relating to the Issuing of DCCKI Certificates are made;

(ii) appropriate backups of the Root DCCKICA are made on a periodic basis;

(iii) backup of cryptographic material used in support of the Root DCCKICA, EII DCCKICA and the UI DCCKICA shall be in line with manufacturer procedures and FIPS 140-2 Level 3 or an equivalent cryptographic standard; and

(iv) security of off-site storage shall be managed and implemented in alignment with security in place at the main locations.

5.2 Procedural controls

5.2.1 Trusted roles

(a) The DCCKICA shall ensure that the DCCKI CPS incorporates provisions designed to ensure that:

(i) Persons with trusted roles are given only the access rights that are commensurate with their role and each has a clearly defined role and access level;

(ii) allocated roles are pertinent to the required task;

(iii) roles and responsibilities are documented;

(iv) no individual member of DCCKICA Personnel is capable, by acting alone, of engaging in any action by means of which the DCCKICA Systems may be Compromised to a material extent;

(v) roles are implemented in line with best practice for a certification authority; and

(vi) multi-person controls are applied with respect to Root DCCKICA Private Key management.

5.2.2 Number of persons required per task

(a) The DCCKICA shall ensure that the DCCKI CPS incorporates provisions designed to establish:

(i) the appropriate separation of roles between the different members of DCCKICA Personnel;

(ii) the application of controls to the actions of all members of DCCKICA Personnel who are Privileged Persons, in particular:

(1) identifying any controls designed to ensure that the involvement of more than one individual is required for the performance of certain functions;

(2) identifying the number of roles that an individual may hold; and

(3) providing that the revocation of any DCCKICA Certificate is one such function; and

(iii) the DCCKICA shall apply such multi-person controls:

(1) in accordance with the operation and risk as identified with within the DCC Information Security Management System;

(2) in accordance with best practice in the case of management of cryptographic material; and

(3) with respect to Root DCCKICA Private Key management.

5.2.3 Identification and authentication for each role

(a) All DCCKICA Personnel shall be required to authenticate via a strong two factor Authentication in accordance with the SMKI PMA Guidance on "Verifying Individual Identity" published on the Website before they can access any facilities.

5.2.4 Roles requiring separation of duties

(a) The DCCKICA shall identify roles that require separation of duties for DCCKICA functions in line with industry best practice.

(b) The DCCKICA shall ensure that the DCCKI CPS incorporates provisions that ensure separation of duties in roles requiring separation of duties.

5.3 Personnel controls

5.3.1 Qualification, experience and clearance requirements

(a) The DCCKICA shall ensure that all DCCKICA Personnel must:

(i) be appointed to their roles in writing;

(ii) be bound by contract to the terms and conditions and non-disclosure agreements relevant to their roles;

(iii) have received appropriate training with respect to their duties; and

(iv) have, as a minimum, passed a Security Check level of vetting, before commencing their roles.

5.3.2 Background check procedures

(a) The DCCKICA shall ensure that all DCCKICA Personnel with access to DCCKICA operations shall undergo formal security checks, as set out within the DCCKI CPS.

5.3.3 Training requirements

(a) See Part 5.3.1 of this Policy.

5.3.4 Retraining frequency and requirements

(a) The DCCKICA shall ensure that the DCCKI CPS incorporates appropriate provisions relating to the frequency and content of retraining and refresher training to be undertaken by DCCKICA Personnel.

5.3.5 Job rotation frequency and sequence

(a) The DCCKICA shall ensure that the DCCKI CPS incorporates appropriate provisions relating to the frequency and sequence of job rotations to be undertaken by DCCKICA Personnel.

5.3.6 Sanctions for unauthorised actions

(a) The DCCKICA shall ensure that the DCCKI CPS incorporates appropriate provisions relating to sanctions for unauthorised actions undertaken by DCCKICA Personnel.

5.3.7 Independent contractor requirements

(a) The DCCKICA shall ensure that all contractors engaged by it adhere to requirements laid out in this Part 5.3.

5.3.8 Documentation supplied to personnel

(a) The DCCKICA shall ensure that all DCCKICA Personnel are provided with access to all documents relevant to their roles or necessary for the performance of their duties, including in particular:

(i) this Policy;

(ii) the DCCKI CPS; and

(iii) any supporting documentation, statutes, policies or contracts.

5.4 Audit logging procedures

5.4.1 Types of events recorded

(a) The DCCKICA shall ensure that:

(i) the DCCKICA Systems record all relevant systems activity in Audit Logs;

(ii) the DCCKI CPS incorporates a comprehensive list of all events that are to be recorded in an Audit Log in relation to the activities of DCCKICA Personnel and the use of DCCKICA equipment which shall include access, both authorised and violations; and

(iii) activities in relation to the DCCKI Registration Authority, are logged in an appropriate manner by the DCCKICA.

5.4.2 Frequency of processing log

(a) DCCKICA audit logging shall:

(i) operate at all times within the DCCKICA Systems; and

(ii) ensure that audit monitoring of the DCCKICA Systems is in compliance with the protective monitoring requirements of DCC Systems.

(b) The DCCKI CPS shall incorporate provisions which specify:

(i) how regularly information recorded in the Audit Log is to be reviewed; and

(ii) what actions are to be taken by the DCCKICA in response to types of events recorded in the Audit Log.

5.4.3 Retention period for Audit Log

(a) The DCCKICA shall retain an Audit Log that incorporates, on any given date, a record of all DCCKICA System events occurring during a period of at least twelve months prior to that date.

(b) A copy of the Audit Log incorporating a record of all system events occurring prior to the beginning of that period shall be archived in accordance with the requirements of Part 5.5 of this Policy.

(c) The DCCKICA shall ensure that the DCCKI CPS makes provision for the specification of the Audit Log record.

5.4.4 Protection of audit log

(a) The DCCKICA shall ensure that the DCCKI CPS incorporates provisions in relation to access to the Audit Log, providing, in particular, that:

(i) access to those DCCKICA Audit Log Data (other than those relating to protective monitoring) must be limited to those members of DCCKICA Personnel who are specifically responsible for performing a system audit role in accordance with the DCCKI CPS;

(ii) to the extent to which the Audit Log is retained electronically, the DCCKICA event log Data stored in it cannot be accessed other than on a read-only basis, and are protected from unauthorised viewing, modification and deletion in accordance with British Standard BS 10008:2014 (Evidential weight and legal admissibility of electronic information) or an equivalent standard; and

(iii) to the extent which the Audit Log is retained in non-electronic form, the Data stored in it are appropriately protected from unauthorised viewing, modification and destruction in order to ensure that their integrity is maintained for evidential purposes.

5.4.5 Audit Log backup procedures

(a) The DCCKICA shall ensure that the Data contained in the Audit Log are backed up on a daily basis or, if activity has taken place on the DCCKICA Systems only infrequently, such as in relation to the Root DCCKICA, in accordance with the schedule for the regular backup of the Data held on those DCCKICA Systems.

(b) The DCCKICA shall ensure that all DCCKI Data contained in the Audit Logs that are backed up are, during backup, held in accordance with the DCC Information Security Management System and protected to the same standard of protection as the primary copy of the Audit Log in accordance with Part 5.4.4 of this Policy.

5.4.6 Audit collection system (internal or external)

(a) The DCCKICA shall ensure that the DCCKI CPS incorporates provisions in relation to its system for collecting Data for the purpose of populating the Audit Log.

5.4.7 Notification to event-causing subject

(a) The DCCKICA shall ensure that the DCCKI CPS incorporates provisions in relation to its notification of any person who is (or is responsible for any DCCKICA System which is) the direct cause of an event recorded in the Audit Log.

5.4.8 Vulnerability assessments

(a) The DCCKICA shall carry out periodic vulnerability assessments covering the DCCKICA Systems with recorded corrective action.

5.5 Records archival

5.5.1 Types of records archived

(a) The DCCKICA shall ensure that it archives:

(i) relevant Audit Data in accordance with Part 5.4 of this Policy;

(ii) records of all Data submitted to it by DCCKI Eligible Subscribers for the purposes of DCCKI Certificate Signing Requests and Personnel Authentication Certificate Applications;

(iii) records of all Data submitted to it by DCCKI Subscribers for the purposes of revocation or suspension of DCCKI Certificates; and

(iv) any other data specified in this Policy as requiring to be archived in accordance with this Part 5.5 of this Policy.

(b) The DCCKICA shall ensure that all DCCKICA audit data are recorded in a standard format that is compliant with British Standard BS 10008:2014 (Evidential Weight and Legal Admissibility of Electronic Information) or an equivalent standard.

(c) The DCCKICA shall ensure that provision is made in the DCCKI CPS in relation to the specification of data to be archived.

5.5.2 Retention period for archive

(a) The DCCKICA shall ensure that all Data, excluding audit data, which are Archived are retained for a period of at least seven years from the date on which they were Archived.

5.5.3 Protection of archive

(a) The DCCKICA shall ensure that Data held in its Archive are protected against any unauthorised access, adequately protected against environmental threats such as temperature, humidity and magnetism and incapable of being modified or deleted.

5.5.4 Archive backup procedures

(a) The DCCKICA shall ensure that the DCCKI CPS incorporates provisions in relation to its procedures for the backup of its Archive.

5.5.5 Requirements for Time-Stamping of records

(a) Provision in relation to Time-Stamping is made in Part 6.8 of this Policy.

5.5.6 Archive collection system (internal or external)

(a) The DCCKICA shall ensure that the DCCKI CPS incorporates provisions in relation to maintaining internal and external archives.

5.5.7 Procedures to obtain and verify archive information

(a) The DCCKICA shall ensure that Data held in the Archive are stored in a readable format during their retention period and that the Data remain accessible at all times during the retention period.

(b) The DCCKICA shall ensure that the DCCKI CPS incorporates provisions in relation to the periodic verification by the DCCKICA of the Data held in the Archive.

5.6 Key changeover

5.6.1 EII DCCKICA key changeover

(a) Where the DCCKICA ceases to use a EII DCCKICA Private Key after the expiry of the Validity Period of a EII DCCKICA Certificate, it shall:

(i) not revoke the related EII DCCKICA Public Key (which may continue to be used for the purpose of checking Digital Signatures generated using the EII DCCKICA Private Key);

(ii) generate a new Key Pair following key generation procedures, generate a DCCKI Certificate Signing Request in relation to the EII DCCKICA Certificate and submit to the Root DCCKICA for signing and Issuance;

(iii) in its role as the DCCKICA:

(1) Issue a new relevant EII DCCKICA Certificate;

(2) confirm acceptance of the EII DCCKICA Certificate once Issued; and

(3) promptly lodge that EII DCCKICA Certificate in the DCCKI Repository;

(iv) ensure that any relevant DCCKI Infrastructure Certificate subsequently Issued by the EII DCCKICA is Issued using the EII DCCKICA Private Key from the newly-generated Key Pair until the expiry of the Validity Period of the newly Issued EII DCCKICA Certificate; and

(v) verifiably destroy the Private Key Material relating to the previous EII DCCKICA Private Key; or retain such Private Key Material in such a manner that it is adequately protected against being put back into use.

5.6.2 UI DCCKICA key changeover

(a) Where the DCCKICA ceases to use a UI DCCKICA Private Key after the expiry of the Validity Period of a UI DCCKICA Certificate, it shall:

(i) not revoke the related UI DCCKICA Public Key (which may continue to be used for the purpose of checking Digital Signatures generated using the UI DCCKICA Private Key);

(ii) generate a new Key Pair following key generation procedures, generate a DCCKI Certificate Signing Request in relation to the UI DCCKICA Certificate, and submit to the Root DCCKICA for signing and Issuance;

(iii) Issue a new relevant UI DCCKICA Certificate in its role as the Root DCCKICA;

(iv) confirm acceptance of the UI DCCKICA Certificate once Issued;

(v) ensure that any relevant Personnel Authentication Certificate subsequently Issued by the UI DCCKICA is Issued using the UI DCCKICA Private Key from the newly-generated Key Pair until the expiry of the Validity Period of the newly Issued UI DCCKICA Certificate; and

(vi) verifiably destroy the Private Key Material relating to the previous UI DCCKICA Private Key; or retain such Private Key Material in such a manner that it is adequately protected against being put back into use.

5.6.3 DCCKI Root Key changeover

(a) Where the Root DCCKICA ceases to use a Root DCCKICA Private Key after the expiry of the Validity Period of a Root DCCKICA Certificate, it shall:

(i) not revoke the related Root DCCKICA Public Key (which may continue to be used for the purpose of checking Digital Signatures generated using the Root DCCKICA Private Key);

(ii) generate a DCCKI Certificate Signing Request for the new Root DCCKICA Certificate and submit it for signing and Issuance;

(iii) issue to itself a new relevant Root DCCKICA Certificate;

(iv) ensure that any relevant EII DCCKICA Certificate or UI DCCKICA Certificate subsequently Issued by the Root DCCKICA is Issued using the Root DCCKICA Private Key from the newly-generated Key Pair until the expiry of the Validity Period of the newly Issued Root DCCKICA Certificate; and

(v) verifiably destroy the Private Key Material relating to the previous Root DCCKICA Private Key; or retain such Private Key Material in such a manner that it is adequately protected against being put back into use.

5.7 Compromise and disaster recovery

5.7.1 Incident and compromise handling procedures

(a) The DCCKICA shall ensure that the DCCKI CPS incorporates Business Continuity and Disaster Recovery Procedures which shall be designed to ensure the continuity or (where there has been unavoidable discontinuity) the recovery of the provision of the DCCKI Services in the event of any Compromise of the DCCKICA Systems or major failure in the DCCKI processes.

(b) In the event of an Incident involving Compromise of the DCCKICA Systems, the DCCKICA shall:

(i) ensure that the Incident Management Policy is invoked;

(ii) not request revocation of any DCCKICA Certificate in the first instance but follow procedures defined in the DCCKI CPS;

(iii) not revoke Issued DCCKI Certificates in the first instance but follow procedures defined in the DCCKI CPS; and

(iv) treat the event as a Major Security Incident.

(c) The DCCKICA shall ensure that the DCCKI CPS incorporates provisions setting out the approach to be taken by it in circumstances in which it suspects (or has reason to suspect) that any EII DCCKICA Private Key or any UI DCCKICA Private Key or any part of the DCCKICA Systems is Compromised.

5.7.2 Computing resources, software and/or data are corrupted

(a) The DCCKICA shall ensure that the DCCKI CPS incorporates provisions in relation to the steps to take to manage computing resources and software, and to deal with corrupted data.

5.7.3 Entity private key compromise procedures

(a) See Part 5.7.1 of this Policy.

5.7.4 Business continuity capabilities after a disaster

(a) The DCCKICA shall ensure that Business Continuity and Disaster Recovery Procedures are invoked in accordance with Part 5.7 of this Policy and the DCCKI CPS.

5.7.5 DCCKICA and DCCKI Registration Authority termination

(a) DCC shall at all times fulfil the functions of the DCCKICA and DCCKI Registration Authority.

6 TECHNICAL SECURITY CONTROLS

(a) The DCCKICA shall ensure that the DCCKI CPS incorporates detailed provision in relation to technical security controls so that such technical security controls are defined, documented and managed for the purpose of exercising its functions as Root DCCKICA, EII DCCKICA, UI DCCKICA and DCCKI Registration Authority.

6.1 Key pair generation and installation

6.1.1 Key pair generation

(a) The DCCKICA shall ensure that all DCCKICA Key Pairs are generated:

(i) in a protected environment to be compliant with FIPS 140-2 Level 3 or an equivalent cryptographic standard;

(ii) using multi-person control, such that no single person is capable of generating any DCCKICA Private Key; and

(iii) in accordance with the DCCKI CPS, with records from the event to be held as archive.

(b) The DCCKICA shall ensure that Key Pairs associated with Personnel Authentication Certificates are generated in accordance with the DCCKI CPS.

(c) The DCCKICA shall not generate any Key Pairs other than a Key Pair associated with a DCCKICA Certificate or a Key Pair associated with a Personnel Authentication Certificate.

6.1.2 Private Key delivery to DCCKI Subscriber

(a) The DCCKICA shall ensure that the DCCKI RAPP makes provision for the generation of a Key Pair associated with a Personnel Authentication Certificate for delivery to a DCCKI Eligible Subscriber by the UI DCCKICA.

6.1.3 Public Key delivery to certificate issuer

(a) The DCCKICA shall ensure that the DCCKI CPS incorporates provisions in relation to the mechanism by which Public Keys of DCCKI Eligible Subscribers are delivered to or generated by, the DCCKICA for the purpose of the exercise of its functions as the Root DCCKICA, EII DCCKICA and UI DCCKICA.

6.1.4 DCCKICA Public Key delivery to Relying Parties

(a) The DCCKICA shall ensure that the DCCKI RAPP incorporates provisions in relation to how Root DCCKICA Public Keys and EII DCCKICA Public Keys shall be delivered to Relying Parties, and in particular that these are placed in the DCCKI Repository following Issuance.

(b) The DCCKICA shall ensure that the DCCKI CPS incorporates provisions in relation to how UI DCCKICA Public Keys shall be delivered to Relying Parties, and in particular that UI DCCKICA Public Keys:

(i) are delivered in a secure fashion and in a manner that precludes substitution attacks;

(ii) may be delivered as specified in a certificate validation or path discovery policy file; and

(iii) that are part of an updated Key Pair may be distributed as a self - signed certificate, and as a new DCCKICA Certificate.

6.1.5 Key sizes

(a) The Root DCCKICA shall employ RSA 4096 bit Private Keys, with a SHA256 hashing algorithm.

(b) The EII DCCKICA shall employ RSA 2048 bit Private Keys, with a SHA256 hashing algorithm.

(c) The UI DCCKICA shall employ RSA 2048 bit Private Keys, with a SHA256 hashing algorithm.

6.1.6 Public Key parameters generation and quality checking

(a) The DCCKICA shall ensure that any Public Key used for the purposes of this Policy shall:

(i) be generated using the required key parameters, as defined in the DCCKI Certificate Profiles in Annex B to this policy, which are in accordance with FIPS 186-4 or an equivalent cryptographic standard; and

(ii) ensure that the quality of the generated key parameters is verified in accordance with FIPS 186-4 or an equivalent cryptographic standard.

6.1.7 Key usage purposes (as per X.509 v3 key usage field)

(a) The DCCKICA shall ensure that each DCCKI Certificate that is Issued by it shall include key usage extension fields that specify the intended use of that DCCKI Certificate and technically limit the certificate's functionality in X.509v3 compliant software.

(b) The DCCKICA shall set key usage bits or assert extended key usage OIDs for each DCCKI Certificate type in accordance with the relevant DCCKI Certificate Profile defined in Annex B to this Policy.

6.2 Private Key Protection and Cryptographic Module Engineering Controls

6.2.1 Cryptographic module standards and controls

(a) The DCCKICA shall ensure that all DCCKICA Private Keys are protected within the cryptographic boundary of a Cryptographic Module configured to be complaint with FIPS 140-2 Level 3 or an equivalent cryptographic standard at all times.

(b) The DCCKICA shall ensure that the key encryption key used to protect the DCCKICA Private Keys is only stored within the cryptographic boundary of a Cryptographic Module configured to be complaint with FIPS 140-2 Level 3 or an equivalent cryptographic standard.

(c) DCCKI Authorised Subscribers shall ensure that all Private Keys provided to them by the DCCKICA or generated by them are protected in accordance with and subject to any conditions specified within Sections G (Security) and L (Smart Metering Key Infrastructure and DCC Key Infrastructure) of the Code, the DCCKI Interface Design Specification and the DCCKI Code of Connection.

6.2.2 Private Key (key (m out of n) multi-person control

(a) The DCCKICA shall ensure that multi-person controls are applied for the generation and management of DCCKICA Private Keys.

(b) DCCKI Authorised Subscribers shall implement multi-person control, where applicable, in accordance with their Information Security Management System.

(c) Private Keys associated with Personnel Authentication Certificates shall not be subject to multi-person control.

6.2.3 Private Key escrow

(a) Key Escrow shall not be used for the DCCKICA.

6.2.4 Private Key backup

(a) The DCCKICA shall back up the DCCKICA Private Keys using multi-person control and shall protect all copies in the same manner as the originals, and in accordance with provisions set out within the DCCKI CPS.

(b) The backup shall be available for use during disaster recovery as described within the DCCKI CPS.

6.2.5 Private Key archival

(a) Private Key archival shall not be implemented for the DCCKICA.

6.2.6 Private Key transfer into or from a Cryptographic Module

(a) The DCCKICA shall ensure that no DCCKICA Private Key is transferred or copied other than:

(i) for the purposes of:

(1) backup;

(2) restoration; or

(3) addition of new hardware, software, or firmware to a Cryptographic Module; and

(ii) in any event, in accordance a level of protection that is compliant with FIPS 140-2 Level 3 or an equivalent cryptographic standard.

(b) The DCCKICA shall ensure that Private Keys associated with Personnel Authentication Certificates:

i. are transferred from the DCCKICA Systems to the systems of DCCKI Eligible Subscribers in a PKCS#12 format and protected with a password; and

ii. following such transfer, that any copies held are verifiably destroyed by the DCCKICA.

(c) The DCCKICA shall ensure that Private Keys associated with Personnel Authentication Certificates for use by Administration Users are generated on a Personal Identity Verification (PIV) compliant Smart Card Token.

6.2.7 Private Key Storage on Cryptographic Module

(a) The DCCKICA shall ensure that DCCKICA Private Keys are stored within the cryptographic boundary of a Cryptographic Module configured to be complaint with FIPS 140-2 Level 3 or an equivalent cryptographic standard.

6.2.8 Method of Activating Private Key

(a) The DCCKICA shall ensure that:

(i) the Cryptographic Module in which any DCCKICA Private Key is stored may be accessed only by an authorised member of DCCKICA Personnel; and

(ii) the requirements of the Cryptographic Module, including switching on and authenticating themselves to the Cryptographic Module shall be undertaken by the DCCKICA Personnel.

6.2.9 Method of deactivating Private Key

(a) The DCCKICA shall ensure that any DCCKICA Private Keys shall be capable of being deactivated by means of the DCCKICA Systems, at least by:

(i) the actions of:

(1) turning off the power;

(2) logging off; or

(3) carrying out a system reset;

or;

(ii) following key changeover in accordance with procedures defined in Part 5.6 of this Policy.

6.2.10 Method of destroying Private Key

(a) The DCCKICA shall ensure that the DCCKI CPS incorporates provisions for a set of procedures covering the destruction of DCCKICA Private Keys and Private Keys associated with Personnel Authentication Certificates delivered to User Personnel of DCCKI Eligible Subscribers. These shall be in accordance with the guidelines provided by the cryptographic manufacturer and compliant with UK Government publication 'IS4 - Management of Cryptographic Systems' or an equivalent cryptographic standard.

(b) The DCCKI CPS shall incorporate provisions for procedures for secure back up of cryptographic material.

(c) Positive decisions on significant key management life cycle events shall be managed directly by the DCCKI PMA.

(d) DCCKI Subscribers shall ensure that their User Information Security Management System includes procedures in relation to the secure management of all Secret Key Material provided to them by the DCCKICA in relation to this Policy. Such procedures shall in particular make provision for:

(i) the security of that Secret Key Material throughout the whole of its lifecycle from its generation to the revocation of the DCCKI Certificate associated with the Secret Key Material; and

(ii) the destruction of any Smart Card Token beyond reasonable use once it is no longer to be used, in accordance with this Policy or as otherwise set out in the Code.

6.2.11 Cryptographic module rating

(a) Any Cryptographic Module used in support of the DCCKICA Systems shall meet the module rating specified within Parts 6.2.1 and 6.2.7 of this Policy.

6.3 Other aspects of Key Pair management

6.3.1 Public Key archival

(a) Public Key archival shall be managed in accordance with Part 5.5 of this Policy and in line with DCCKI Repository management requirements as detailed within the DCCKI CPS.

6.3.2 Certificate operational periods and Key Pair usage periods

(a) Annex B to this Policy specifies the detail for Key Pair usage, Validity Period and categories.

(b) The DCCKICA shall ensure that the Validity Period of each DCCKI Certificate Issued by it shall be as follows:

(i) in the case of a Root DCCKICA Certificate, 20 years;

(ii) in the case of a EII DCCKICA Certificate, or UI DCCKICA Certificate, 10 years; and

(iii) in the case of a DCCKI Infrastructure Certificate or Personnel Authentication Certificate, 3 years.

(c) The DCCKICA shall ensure that no DCCKICA Private Key can be used after the end of the Validity Period of the DCCKICA Certificate containing the Public Key which is associated with that Private Key.

6.4 Activation Data

6.4.1 Activation data generation and installation

(a) The DCCKICA shall ensure that any Cryptographic Module within which a DCCKICA Private Key is held has Activation Data that apply sufficient security protection to protect that DCCKICA Private Key.

(b) Activation Data pertaining to the DCCKICA Private Key Material shall:

(i) have access controls applied as defined within the DCCKI CPS;

(ii) have key management lifecycle procedures applied as defined within the DCCKI CPS; and

(iii) have records generated, logged and archived on generation and each invocation.

6.4.2 Activation data protection

(a) The DCCKICA shall ensure that the DCCKI CPS incorporates provisions in relation to the physical and logical controls to be employed to protect activation data.

6.5 Computer security controls

6.5.1 Specific computer security technical requirements

(a) The DCC Information Security Management System shall define security technical requirements according to a risk assessment and risk treatment plan, or following corrective action that may result from an audit or IT health check service, which shall be undertaken by a CESG CHECK service provider.

6.5.2 Computer security rating

(a) This Policy makes no stipulation in relation to computer security rating.

6.6 Life cycle technical controls

6.6.1 System development controls

(a) The DCCKICA shall ensure that the DCCKI CPS makes provision regarding controls in relation to development of the DCCKICA Systems; and

(b) any such development of the DCCKICA Systems shall be made in accordance with DCC secure development policy as defined within the DCC Information Security Management System.

6.6.2 Security management controls

(a) The DCCKICA shall ensure that the DCCKI CPS, incorporates provisions which are designed to ensure that the DCCKICA Systems satisfy the requirements of Section G2 (System Security: Obligations on the DCC) and Section G5 (Information Security: Obligations on the DCC and Users) of the Code.

6.6.3 Life cycle security controls

(a) See Part 6.6.2 of this Policy.

6.7 Network security controls

6.7.1 Protection against attack

(a) The DCCKICA shall ensure that the DCCKICA systems are protected against attack in accordance with provisions made in the DCCKI CPS and by at least the following means:

(i) continual protective monitoring shall be enforced; and

(ii) access to the systems shall be on a least privilege principle for access.

(b) The DCCKICA Systems shall be designed and operated so as to detect and prevent:

(i) Denial of Service Events; and

(ii) unauthorised attempts to connect to them.

6.7.2 Health Check of DCCKICA Systems

(a) The DCCKICA shall ensure that the DCCKI CPS incorporates provisions for periodically scheduled assessments of the DCCKICA Systems by a CESG CHECK service provider to form part of the input to the risk management process.

6.8 Time-stamping

6.8.1 Use of time-stamping

(a) The DCCKICA shall ensure Time-Stamping takes place in relation to all DCCKI Certificates and other DCCKI activities that require an accurate record of time.

(b) The DCCKICA shall ensure that the DCCKI CPS incorporates provisions in relation to the time source and mechanisms used by any Time-Stamping Authority in relation to any Time-Stamping on behalf of the DCCKICA.

7 CERTIFICATE, CRL, AND OCSP PROFILES

7.1 Certificate profile

(a) The DCCKICA shall only issue certificates in accordance with the DCCKI Certificate Profiles in Annex B of this Policy for Service Users and the DCCKI Certificate Profiles in Annex C of the DCCKI CPS for Service Providers.

7.1.1 Version number(s)

(a) The version field in the DCCKI Certificates shall have a value of 2, indicating X.509v3 certificates.

7.1.2 Certificate extensions

(a) In compliance with RFC 5280, the inclusion of the following certificate extensions shall be utilised:

(i) authorityKeyIdentifier NOT CRITICAL;

(ii) authorityInfoAccess NOT CRITICAL, for EII DCCKICA Certificates, DCCKI Infrastructure Certificates and Personnel Authentication Certificates only;

(iii) basicConstraints CRITICAL;

(iv) extKeyUsage NOT CRITICAL;

(v) keyUsage CRITICAL;

(vi) certificatePolicies NOT CRITICAL;

(vii) cRLDistributionPoints NOT CRITICAL;

(viii) subjectAltName NOT CRITICAL;

(ix) subjectKeyIdentifier NOT CRITICAL.

7.1.3 Algorithm object identifiers

(a) No stipulation.

7.1.4 Name forms

(a) The DCCKI CPS sets out the name forms utilised.

7.1.5 Name constraints

(a) The DCCKI CPS sets out the applicable Name Constraints.

7.1.6 Certificate policy object identifier

(a) No stipulation.

7.1.7 Usage of Policy Constraints extension

[Not applicable].

7.1.8 Policy qualifiers syntax and semantics

[Not applicable].

7.1.9 Processing semantics for the critical Certificate Policies extension

[Not applicable].

7.2 CRL profile

7.2.1 Version number(s)

(a) The version field in the certificate shall state 1, indicating X.509v2 CRL.

7.2.2 CRL and CRL entry extensions

(a) No stipulation.

7.3 OCSP profile

(a) The DCCKICA shall not employ an OCSP.

7.3.1 Version number(s)

[Not applicable].

7.3.2 OCSP extensions

[Not applicable].

8 COMPLIANCE AUDIT AND OTHER ASSESSMENTS

(a) The DCC Information Security Management System shall include provisions relating to the compliance and audit of the DCCKICA, and DCCKICA Systems that shall be in accordance with relevant provisions made in Section G (Security) of the Code.

8.1 Frequency or circumstances of assessment

(a) The DCCKICA shall be subject to assessment schedules set out in the DCC Information Security Management System, with such assessments taking place at least annually.

8.2 Identify/qualifications of assessor

(a) In accordance with the DCC Information Security Management System, the DCCKICA shall be subject to independent assessment by a UKAS approved certification body whose qualifications shall include ISO/IEC 27001 Lead Audit and IRCA Registration.

8.3 Assessor's relationship to assessed entity

(a) Any UKAS approved certification body carrying out independent assessments shall be subject to UKAS scrutiny with regards to independence of the chosen assessor.

8.4 Topics covered by assessment

(a) The DCC Information Security Management System shall cover all aspects of the DCCKI Service and the DCCKI Repository Service, including but not limited to:

(i) the DCCKI Repository;

(ii) the Root DCCKICA;

(iii) the UI DCCKICA;

(iv) the EII DCCKICA;

(v) The DCCCKI Registration Authority;

(vi) Cryptographic Modules relied upon in support of the service; and

(vii) this Policy and its supporting DCCKI RAPP and DCCKI CPS.

8.5 Actions taken as a result of deficiency

(a) Any deficiencies identified through third party assessment, internal audit or IT health check shall be raised by DCC as non-conformances and be processed through risk assessment and processes defined within the DCC Information Security Management System.

8.6 Communication of results

(a) The DCCKICA shall make the results of corrective action available to the DCCKI PMA.

9 OTHER BUSINESS AND LEGAL MATTERS

(a) In so far as provision is made in relation to all the matters referred to in this Part, it is found in the DCC Licence and the provisions of the Code.

9.1 Fees

[Not applicable].

9.1.1 Certificate Issuance or renewal fees

[Not applicable].

9.1.2 Device certificate access fees

[Not applicable].

9.1.3 Revocation or status information access fees

[Not applicable].

9.1.4 Fees for other services

[Not applicable].

9.1.5 Refund policy

[Not applicable].

9.2 Financial responsibility

9.2.1 Insurance coverage

(a) See the statement at the beginning of this Part.

9.2.2 Other assets

(a) See the statement at the beginning of this Part.

9.2.3 Insurance or warranty coverage for subscribers and subjects

(a) See the statement at the beginning of this Part.

9.3 Confidentiality of business information

9.3.1 Scope of confidential information

(a) See the statement at the beginning of this Part.

9.3.2 Information not within the scope of confidential information

(a) See the statement at the beginning of this Part.

9.3.3 Responsibility to protect confidential information

(a) See the statement at the beginning of this Part.

9.4 Privacy of personal information

9.4.1 Privacy plan

(a) See the statement at the beginning of this Part.

9.4.2 Information treated as private

(a) See the statement at the beginning of this Part.

9.4.3 Information not deemed private

(a) See the statement at the beginning of this Part.

9.4.4 Responsibility to protect private information

(a) See the statement at the beginning of this Part.

9.4.5 Notice and consent to use private information

(a) See the statement at the beginning of this Part.

9.4.6 Disclosure pursuant to judicial or administrative process

(a) See the statement at the beginning of this Part.

9.4.7 Other information disclosure circumstances

(a) See the statement at the beginning of this Part.

9.5 Intellectual property rights

(a) See the statement at the beginning of this Part.

9.6 Representations and warranties

9.6.1 CA representations and warranties

(a) See the statement at the beginning of this Part.

9.6.2 RA representation and warranties

(a) See the statement at the beginning of this Part.

9.6.3 Subscriber representations and warranties

(a) See the statement at the beginning of this Part.

9.6.4 Relying party representations and warranties

(a) See the statement at the beginning of this Part.

9.7 Representations and warranties of other participants

(a) See the statement at the beginning of this Part.

9.8 Disclaimers of warranties

(a) See the statement at the beginning of this Part.

9.9 Limitations of liability

(a) See the statement at the beginning of this Part.

9.10 Indemnities

(a) See the statement at the beginning of this Part.

9.11 Term and termination

9.11.1 Term

(a) See the statement at the beginning of this Part.

9.11.2 Termination

(a) See the statement at the beginning of this Part.

9.11.3 Effect of termination and survival

(a) See the statement at the beginning of this Part.

9.12 Individual notices and communications with participants

(a) See the statement at the beginning of this Part.

9.13 Amendments

9.13.1 Procedure for amendment

(a) See the statement at the beginning of this Part.

9.13.2 Notification mechanism and period

(a) See the statement at the beginning of this Part.

9.13.3 Circumstances under which OID must be changed

(a) See the statement at the beginning of this Part.

9.14 Dispute resolution provisions

(a) See the statement at the beginning of this Part.

9.15 Governing law

(a) See the statement at the beginning of this Part.

9.16 Compliance with applicable law

(a) See the statement at the beginning of this Part.

9.17 Miscellaneous provisions

9.17.1 Entire agreement

(a) See the statement at the beginning of this Part.

9.17.2 Assignment

(a) See the statement at the beginning of this Part.

9.17.3 Severability

(a) See the statement at the beginning of this Part.

9.17.4 Enforcement (attorneys' fees and waiver of rights)

(a) See the statement at the beginning of this Part.

9.17.5 Force Majeure

[Not applicable].

9.18 Other provisions

(a) See the statement at the beginning of this Part.

ANNEX A

DEFINED TERMS

In this Policy, except where the context otherwise requires:

- expressions defined in Section A (Definitions and Interpretation) of the Code have the same meaning as is set out in that section;
- the expressions in the left hand column below shall have the meanings given to them in the right hand column below; and
- where any expression is defined in Section A (Definitions and Interpretation) of the Code and in this Annex, the definition in this Annex shall take precedence for the purposes of the Policy.

Definitions for this Policy

Administration User	has the meaning given to the term Administration User in Appendix AI of the Code (Self Service Interface Code of Connection)
Archive	means the archive of Data created in accordance with Part 5.5.1 of this Policy (and "Archives" and "Archived" shall be interpreted accordingly)
Audit Log	means the audit log created in accordance with Part 5.4.1 of this Policy
Authentication	means the process of establishing that an individual, DCCKI Certificate, system or organisation is who or what they or it claims or is claimed to be (and “Authenticate” shall be interpreted accordingly)
Business Continuity and Disaster Recovery Procedure	means that part of the Incident Management Policy which describes the business continuity and disaster recovery procedures applicable to the DCCKI Services.
Certificate Re-Key	means a change to the Public Key contained within a Certificate bearing a particular serial number.
DCCKI Authorised Responsible Officer (or **DCCKI ARO)**	means an individual that has successfully completed the process for becoming (and remains) a DCCKI ARO on behalf of a Party or RDP in accordance with the DCCKI RAPP.
DCCKI Authorised Subscriber	means (in relation to DCCKICA Certificates), the DCC or (in relation to DCCKI Infrastructure Certificates and Personnel Authentication Certificates), a Party or Registration Data Provider that: i. has successfully completed the enrolment procedures to become a DCCKI Authorised Subscriber as set out in the DCCKI RAPP; ii. continues to have at least one (1) DCCKI SRO currently appointed in accordance with the procedures set out in the DCCKI RAPP; iii. continues to have at least one (1) DCCKI ARO currently appointed in accordance with the procedures set out in the DCCKI RAPP; iv. has not ceased to be a DCCKI Authorised Subscriber in accordance with any other provision of the Code and in the case of the DCC only, subject to any alternative provisions in the DCCKI CPS.
DCCKI Authority Revocation List (or DCCKI ARL)	means a list, produced by the Root DCCKICA, of all EII DCCKICA Certificates that have been revoked in accordance with this Policy.
DCCKI Certificate	has the meaning given to that expression in Part 1.1 of this Policy
DCCKI Certificate Profile	means a table bearing that title in Annex B to this Policy and specifying the parameters to be contained within a DCCKI Certificate

DCCKI Certificate Revocation Request	means a request for the revocation of a DCCKI Certificate by the DCCKICA, submitted by the DCCKI Subscriber for that DCCKI Certificate to the DCCKICA in accordance with the DCCKI RAPP and this Policy.
DCCKI Certification Authority (or DCCKICA)	means the Certification Authority for the DCCKI, meaning the DCC, acting in this capacity and exercising the functions of a. the Root DCCKICA; b. the EI DCCKICA; c. the UI DCCKICA; and d. the DCCKI Registration Authority.
DCCKI Infrastructure Certificate	means a certificate in the form set out in the DCCKI Infrastructure certificate profile in accordance with Annex B to this Policy, and Issued by the EII DCCKICA in accordance with this Policy or the DCCKI CPS for the purposes set out in Part 1.4.1 (e) of this Policy.
DCCKI Policy Management Authority (or DCCKI PMA)	means the DCC acting in this capacity for the purposes of administering this Policy and related matters.
DCCKI Registration Authority	means the DCCKI CA exercising the function of receiving and processing DCCKI Certificate Signing Requests and Personnel Authentication Certificate Applications made in accordance with the DCCKI RAPP.
DCCKI Registration Authority Manager	means any person who may be identified as such in accordance with the DCCKI RAPP.
DCCKI Registration Authority Personnel	means those persons who are engaged by the DCC, in so far as such persons carry out, or are authorised to carry out, any function of the DCCKI Registration Authority.
DCCKI Senior Responsible Officer (or **DCCKI SRO)**	means an individual that has successfully completed the process for becoming (and remains) a DCCKI SRO on behalf of a Party, or RDP in accordance with the DCCKI RAPP.
DCCKICA Certificate	means, as the context requires, either: (a) the Root DCCKICA Certificate; (b) an EII DCCKICA Certificate; or (c) an UI DCCKICA Certificate.
DCCKICA Personnel	means those persons who are engaged by the DCC, in so far as such persons carry out, or are authorised to carry out, any function of the DCCKICA.
DCCKICA Private Key	means a Private Key which is stored by the DCCKICA acting in its capacity as either the Root DCCKICA, the EII DCCKICA or the UI DCCKICA.
DCCKICA Systems	means the Systems used by the DCCKICA in relation to the DCCKI Services.

EII DCCKICA	means the External Infrastructure Issuing Authority, being a subordinate Issuing Authority for the DCCKICA whose functions are carried out by the DCCKICA.
EII DCCKICA Certificate	means a certificate of the form set out in the EII DCCKICA Certificate DCCKI Certificate Profile in accordance with Annex B to this Policy, and Issued by the Root DCCKICA to the EII DCCKICA in accordance with this Policy.
EII DCCKICA Certificate Revocation List (or EII DCCKICA CRL)	means a list, produced by the EII DCCKICA, of all DCCKI Infrastructure Certificates that have been revoked in accordance with this Policy.
EII DCCKICA Private Key	means a Private Key which is stored and managed by the DCCKICA acting in its capacity as the EII DCCKICA.
EII DCCKICA Public Key	means the Public Key of a Key Pair related to a EII DCCKICA Certificate.
Identity Provider Service	has the meaning given to that term in the Self Service Interface Code of Connection.
IRCA	International Register of Certificated Auditors, a professional body for management system auditors.
Issue	means the act of the DCCKICA acting in accordance with this Policy, and in its capacity as the Root DCCKICA, the EII DCCKICA or the UI DCCKICA as the context requires, of creating and signing a Certificate which contains the information set out in the relevant DCCKI Certificate Profile in Annex B to this Policy (and “Issuance”, “Issued” and “Issuing” shall be interpreted accordingly).
Key Escrow	means the storage of a Private Key by a person other than the Subscriber or Subject of the Certificate which contains the related Public Key.
Object Identifier (or **OID**)	means an object identifier assigned by the Internet Address Naming Authority.
Personal Identity Verification	a Smart Card Token compliant with Federal Information Processing Standard (FIPS) 201.
Personnel Authentication Certificate	means a certificate in the form set out in the Personnel Authentication Certificate DCCKI Certificate Profile in Annex B to this Policy, and Issued by the UI DCCKICA in accordance with this Policy.
Personnel Authentication Certificate Application	means an application for a Personnel Authentication Certificate made via the Personnel Credentials Interface.

Personnel Credentials Interface	means the interface that allows for the activation of user accounts, the submission of Personnel Authentication Certificate Applications, and the provision of Personnel Authentication Certificates to persons.
Private Key Material	in relation to a Private Key, means that Private Key and the input parameters necessary to establish, use and maintain it.
Root DCCKICA	means the DCC exercising the function of Issuing the Root DCCKI Certificate and other DCCKI CA Certificates to the EI DCCKICA and UIDCCKI, and storing and managing Private Keys associated with that function.
Root DCCKICA Certificate	means a certificate of the form set out in the Root DCCKI Certificate DCCKI Certificate Profile in accordance with Annex A of this Policy and self-signed, and Issued, by the Root DCCKICA in accordance with this Policy.
Root DCCKICA Private Key	means the Private Key which is stored and managed by the DCCKICA acting in its capacity as the Root DCCKICA.
Root DCCKICA Public Key	means the Public Key of a Key Pair related to the Root DCCKICA Certificate.
SAML	means Security Assertion Markup Language, being a standard that allows secure web domains to exchange user authentication and authorisation data.
Security Related Functionality	means the functionality of the DCCKICA Systems which is designed to detect, prevent or mitigate the adverse effect of any Compromise of those Systems.
Smart Card Token	a physical security device used to assist authentication of User Personnel
Subject	means: a. in relation to a DCCKI Infrastructure Certificate, the Organisation identified in the 'Subject Name' field of the DCCKI Infrastructure Certificate DCCKI Certificate Profiles in Annex B to this Policy; b. in relation to a Personnel Authentication Certificate, the person identified in the 'Subject Name' field of the Personnel Authentication Certificate DCCKI Certificate profile in Annex B to this Policy; or c. in relation to an DCCKICA Certificate, the globally unique name of the Root DCCKICA, EII DCCKICA, or UI DCCKICA as identified in the 'Subject' field of the relevant DCCKI Certificate Profile in Annex B to this Policy.
Time-Stamping	means the act that takes place when a Time-Stamping Authority, in relation to a DCCKI Certificate, stamps a particular datum with an accurate indicator of the time (in hours, minutes and seconds) at which the activity of stamping takes place.

Time-Stamping Authority	means that part of the DCCKICA that: a. where required, provides an appropriately precise time-stamp in the format required by this Policy; and b. relies on a time source that is: i. accurate; ii. determined in a manner that is independent of any other part of the DCCKICA Systems; and iii. such that the time of any time-stamp can be verified to be that of the Independent Time Source at the time at which the time-stamp was applied.
Transport Layer Security (or TLS)	means TLS in accordance with the relevant SMKI PMA and SSC Guidance (Standards, Procedures and Guidelines) published on the SEC website
UI DCCKICA	means the User Issuing Authority, being a subordinate Issuing Authority for the DCCKICA whose functions are carried out by the DCCKICA.
UI DCCKICA Certificate	means a certificate in the form set out in the UI DCCKICA Certificate DCCKI Certificate Profile in accordance with Annex B to this Policy, and Issued by the Root DCCKICA to the UI DCCKICA in accordance with this Policy.
UI DCCKICA Private Key	means a Private Key which is stored and managed by the DCCKICA acting in its capacity as the UI DCCKICA.
UI DCCKICA Public Key	means the Public Key of a Key Pair related to a UI DCCKICA Certificate.
Validity Period	means, in respect of a DCCKI Certificate, the period of time for which that DCCKI Certificate is intended to be valid.

ANNEX B

DCCKI CERTIFICATE PROFILES

End Entity Certificate Structure and Contents

This Annex B sets out requirements as to structure and content with which DCCKICA Certificates, DCCKI Infrastructure Certificates, and Personnel Authentication Certificates shall comply. All terms in this Annex shall, where not defined in the Code, this Policy, or the GB Companion Specification, have the meanings in and IETF RFC 5280.

Common Requirements applicable to all DCCKI Certificates

All DCCKI Certificates that are validly authorised within the DCCKI shall:

- Be an X.509 v3 certificate;

- Have a Serial number of no more than 20 octets;
- have a valid notBefore field consisting of the time of issue, encoded as in section 4.1.2.5 of RFC 5280;
- have a fixed expiration date in the notAfter field, encoded as in section 4.1.2.5 of RFC 5280; and
- Contain an authorityKeyIdentifier and subjectKeyIdentifier in the form [0] KeyIdentifier. This extension shall be marked as non-critical, and calculated using method 2 of section 4.2.1.2 of RFC 5280.

Requirements applicable to DCCKI Infrastructure Certificates only

A DCCKI Infrastructure Certificate that is Issued by the EII DCCKICA for the purposes of establishing Transport Layer Security (TLS) and File Transfer Protocol over TLS (FTPS) communications over a DCC Gateway Connection shall:

- have a keyUsage extension (as per section 4.2.1.3 of RFC 5280) with a value of digitalSignature, and keyEncipherment. This extension shall be marked as critical (as per section 4.2.1.3 of RFC 5280);
- have an extendedKeyUsage extension (as per section 4.2.1.12 of RFC 5280) with a value of id-kp-serverAuth and id-kp-clientAuth. This extension shall be marked as non-critical;
- contain a single policyIdentifier in the certificatePolicies extension that refers to the OID for the DCCKI Certificate Policy; and
- have a Validity Period of 3 years.

A DCCKI Infrastructure Certificate that is Issued by the EII DCCKICA for the purposes of establishing SAML assertions to the DCC shall:

- have a keyUsage extension (as per section 4.2.1.3 of RFC 5280) with a value of digitalSignature, this extension shall be marked as critical (as per section 4.2.1.3 of RFC 5280);
- contain a single policyIdentifier in the certificatePolicies extension that refers to the OID for the DCCKI Certificate Policy; and
- have a Validity Period of 3 years.

Requirements Applicable to Personnel Authentication Certificates (ordinary users) only

Personnel Authentication Certificates that are issued by the UI DCCKICA for the purposes of Authenticating User Personnel to the Self Service Interface shall:

- have a keyUsage extension (as per section 4.2.1.3 of RFC 5280) with a value of digitalSignature. This extension shall be marked as critical (as per section 4.2.1.3 of RFC 5280);
- contain a single policyIdentifier in the certificatePolicies extension that refers to the OID for the DCCKI Certificate Policy;
- contain an authorityKeyIdentifier in the form [0] KeyIdentifier. This shall be generated using method (2) of section 4.2.1.2 of RFC 5280. This extension shall be marked as non-critical;

- include the Subject name as a meaningful name or other means of identifying an individual as provided by the DCCKI Eligible Subscriber; and
- have a Validity Period of 3 years.

Requirements Applicable to Personnel Authentication Certificates only

Personnel Authentication Certificates that are issued by the UI DCCKICA for the purposes of Authenticating Administration Users to the Self Service Interface shall:

- have a keyUsage extension (as per section 4.2.1.3 of RFC 5280) with a value of digitalSignature. This extension shall be marked as critical (as per section 4.2.1.3 of RFC 5280);
- contain a two policyIdentifier in the certificatePolicies extension that refers to the OID for the DCCKI Certificate Policy and the OID for validation policy of the Smart Card Token PIV Authentication Key;
- contain an authorityKeyIdentifier in the form [0] KeyIdentifier. This shall be generated using method (2) of section 4.2.1.2 of RFC 5280. This extension shall be marked as non-critical;
- include the Subject name as a meaningful name or other means of identifying an individual as provided by the DCCKI Eligible Subscriber; and
- have a Validity Period of 3 years.

Requirements Applicable to EII DCCKICA and UI DCCKICA Certificates only

An EII DCCKICA Certificate or UI DCCKICA Certificate issued by the Root DCCKICA shall:

- have a keyUsage extension (as per section 4.2.1.3 of RFC 5280) with a value of keyCertSign, Offline CRL Signing and cRLSign. This extension shall be marked as critical (as per section 4.2.1.3 of RFC 5280);
- contain at least one policyIdentifier in the certificatePolicies extension that refers to the OID for the DCCKI Certificate Policy;
- contain the basicConstraints extension, with values cA=True, and pathLen=0. This extension shall be marked as critical; and
- have a Validity Period of 10 years.

Requirements Applicable to Root DCCKICA Certificates only

Root DCCKICA Certificates that are issued by the Root DCCKICA shall:

- have a keyUsage extension (as per section 4.2.1.3 of RFC 5280) with a value of keyCertSign, Offline CRL Signing and cRLSign. This extension shall be marked as critical (as per section 4.2.1.3 of RFC 5280);
- contain a single policyIdentifier in the certificatePolicies extension that refers to the OID for anyPolicy;

- contain the basicConstraints extension, with values cA=True, and pathLen absent (unlimited). This extension shall be marked as critical; and
- have a Validity Period of 20 years.

DCCKI Infrastructure Certificate DCCKI Certificate Profile for the purposes of establishing TLS Communications

Field Name	RFC 5759/5280 Type	Value	Reference
Version	Integer	V3	
serialNumber	Integer	calculated by CA	
signatureAlgorithm		rsa-withSHA256	
Issuer	Name	CN= EII DCCKICA, O=DCC, C=UK	
notBefore	Time	Calculated by CA as time of issue	
notAfter	Time	Calculated by CA as not before + 3 years	
Subject	Name	CN=<FQDN>, O= Party or RDP Signifier, C=UK	
subjectPublicKeyInfo		RSA	
keyLength		2048 bits	
Extensions	Extensions	Critical and non-critical extensions	
authorityKeyIdentifier	KeyIdentifier	Calculated by CA	
subjectKeyIdentifier	KeyIdentifier	Calculated by CA	
keyUsage		digitalSignature, keyEncipherment	
certificatePolicies		1.2.826.0.1.8641679.1.2.1.1 1	

extendedKeyUsage		id-kp-serverAuth, id-kp-clientAuth	
applicationPolicies		Server Authentication Client Authentication	
cRLDistributionPoint	http location	[1] http://dcckirepo.prod.dsp.dccinterface.co.uk/revocationlists/download/EIIDCCKICA-00.crl	
authorityInfoAccess	http location	[1] http://dcckirepo.prod.dsp.dccinterface.co.uk/certificatesearch/downloadcert/EIIDCCKICA-00.crt	

Interpretation

Version

The version of the X.509 DCCKI Infrastructure Certificate. DCCKI Infrastructure Certificates shall identify themselves as version 3.

serialNumber

DCCKI Infrastructure Certificate serial number, a positive integer of no more than 20 octets. The Serial Number identifies the DCCKI Infrastructure Certificate, and shall be created by the Issuing EII DCCKICA that signs the DCCKI Infrastructure Certificate. The Serial Number shall be unique in the scope of DCCKI Infrastructure Certificates signed by the Issuing EII DCCKICA.

signatureAlgorithm

The identity of the signature algorithm used to sign the DCCKI Infrastructure Certificate. The field shall be rsa-with-SHA256 as defined in NIST FIPS 180-4.

Issuer

The name of the signer of the DCCKI Infrastructure Certificate. This will consist of the Country (C), Organisation Name (O) which will be DCC and a Common Name (CN) which will be EII DCCKICA (as defined in the EII DCCKICA Certificate profile).

Validity

The time period over which the EII DCCKICA expects the DCCKI Infrastructure Certificate to be valid. The validity period is the period of time from notBefore through notAfter, inclusive.

All times shall be stated in the Universal Coordinated Time (UTC) time zone. Time up to and including 23:59:59 December 31, 2049 UTC shall be encoded as UTCTime as YYMMDDHHmmssZ.

Times later than 23:59:59 December 31, 2049 UTC shall be encoded as GeneralizedTime as YYYYMMDDHHmmssZ.

notBefore

The earliest time a DCCKI Infrastructure Certificate may be used. This shall be the time the DCCKI Infrastructure Certificate is created.

notAfter

The latest time a DCCKI Infrastructure Certificate is expected to be used. The value in a notAfter field shall be treated as specified in RFC 5280.

Subject

The formatting of this field shall contain a unique X.500 Distinguished Name (DN). This shall consist of the Country (C), the Organisation Name (O) which will be the Party Signifier or RDP Signifier of the DCCKI Subscriber who is also a SMKI Subscriber and a Common Name (CN) which will be the Fully Qualified Domain Name of the DCCKI Subscriber.

subjectKeyPublicInfo

The Key Algorithm shall be RSA as defined in NIST FIPS 186-4.

keyLength

The Key length shall be RSA 2048 bits.

Extensions

DCCKI Infrastructure Certificates MUST contain the extensions described below. They SHOULD NOT contain any additional extensions:

- authorityKeyIdentifier
- subjectKeyIdentifier
- applicationPolicies
- keyUsage: critical
- certificatePolicies: non critical
- extendedKeyUsage: non-critical
- cRLDistributionPoint
- authorityInfoAccess

authorityKeyIdentifier

A key identifier calculated using method 2 of section 4.2.1.2 of RFC 5280.

subjectKeyIdentifier

Calculated using method 2of section 4.2.1.2 of RFC 5280.

keyUsage

As per RFC 5280 section 4.2.1.3 with a value of digitalSignature, and keyEncipherment.

certificatePolicies

Contain a single policyIdentifier in the certificatePolicies extension that refers to the OID for the DCCKI Certificate Policy.

extendedKeyUsage

This shall be an extendedKeyUsage extension (as per section 4.2.1.12 of RFC 5280) with a value of id-kp-serverAuth and id-kp-clientAuth. This extension shall be marked as non-critical.

applicationPolicies

This shall be populated with the following policy identifies, Server Authentication and Client Authentication. This extension shall be marked as non-critical.

cRLDistributionPoint

URI string, which shall identify the URL of the EII DCCKICA CRL within the DCCKI Repository. This extension shall be marked as non-critical.

authorityInfoAccess

URI string, which shall identify where to access information and services for the EII DCCKICA within the DCCKI Repository. This extension will be marked as non-critical.

DCCKI Infrastructure Certificate DCCKI Certificate Profile for the purposes of establishing FTPS Communications

Field Name	RFC 5759/5280 Type	Value	Reference
Version	Integer	V3	
serialNumber	Integer	calculated by CA	
signatureAlgorithm		rsa-withSHA256	
Issuer	Name	CN= EII DCCKICA, O=DCC, C=UK	

notBefore	Time	Calculated by CA as time of issue	
notAfter	Time	Calculated by CA as not before + 3 years	
Subject	Name	CN=<Party or RDP Signifier>	
subjectPublicKeyInfo		RSA	
keyLength		2048 bits	
Extensions	Extensions	Critical and non-critical extensions	
authorityKeyIdentifier	KeyIdentifier	Calculated by CA	
subjectKeyIdentifier	KeyIdentifier	Calculated by CA	
keyUsage		digitalSignature, keyEncipherment	
certificatePolicies		1.2.826.0.1.8641679.1.2.1.11	
subjectAltName		<Fully Qualified Domain Name>	
extendedKeyUsage		id-kp-serverAuth, id-kp-clientAuth	
applicationPolicies		Server Authentication Client Authentication	
cRLDistributionPoint	http location	[1] http://dcckirepo.prod.dsp.dccinterface.co.uk/revocationlists/download/EIIDCCKICA-00.crl	
authorityInfoAccess	http location	[1] http://dcckirepo.prod.dsp.dccinterface.co.uk/certificatesearch/downloadcert/EIIDCCKICA-00.crt	

Interpretation

Version

The version of the X.509 DCCKI Infrastructure Certificate. DCCKI Infrastructure Certificates shall identify themselves as version 3.

serialNumber

DCCKI Infrastructure Certificate serial number, a positive integer of no more than 20 octets. The Serial Number identifies the DCCKI Infrastructure Certificate, and shall be created by the Issuing EII DCCKICA that signs the DCCKI Infrastructure Certificate. The Serial Number shall be unique in the scope of DCCKI Infrastructure Certificates signed by the Issuing EII DCCKICA.

signatureAlgorithm

The identity of the signature algorithm used to sign the DCCKI Infrastructure Certificate. The field shall be rsa-with-SHA256 as defined in NIST FIPS 180-4.

Issuer

The name of the signer of the DCCKI Infrastructure Certificate. This will consist of the Country (C), Organisation Name (O) which will be DCC and a Common Name (CN) which will be EII DCCKICA (as defined in the EII DCCKICA Certificate profile).

Validity

The time period over which the EII DCCKICA expects the DCCKI Infrastructure Certificate to be valid. The validity period is the period of time from notBefore through notAfter, inclusive.

All times shall be stated in the Universal Coordinated Time (UTC) time zone. Time up to and including 23:59:59 December 31, 2049 UTC shall be encoded as UTC Time as YYMMDDHHmmssZ.

Times later than 23:59:59 December 31, 2049 UTC shall be encoded as Generalized Time as YYYYMMDDHHmmssZ.

notBefore

The earliest time a DCCKI Infrastructure Certificate may be used. This shall be the time the DCCKI Infrastructure Certificate is created.

notAfter

The latest time a DCCKI Infrastructure Certificate is expected to be used. The value in a notAfter field shall be treated as specified in RFC 5280.

Subject

The formatting of this field shall contain a unique X.500 Distinguished Name (DN). This shall consist of a Common Name (CN) shall be populated with the Party Signifier or RDP Signifier of the DCCKI Subscriber.

subjectKeyPublicInfo

The Key Algorithm shall be RSA as defined in NIST FIPS 186-4.

keyLength

The Key length shall be RSA 2048 bits.

Extensions

DCCKI Infrastructure Certificates MUST contain the extensions described below. They SHOULD NOT contain any additional extensions:

- authorityKeyIdentifier
- subjectKeyIdentifier
- applicationPolicies
- keyUsage: critical
- certificatePolicies: non critical
- subjectAltName: non-critical
- extendedKeyUsage: non-critical
- cRLDistributionPoint
- authorityInfoAccess

authorityKeyIdentifier

A key identifier calculated using method 2 of section 4.2.1.2 of RFC 5280.

subjectKeyIdentifier

Calculated using method 2of section 4.2.1.2 of RFC 5280.

keyUsage

As per RFC 5280 section 4.2.1.3 with a value of digitalSignature and keyEncipherment.

certificatePolicies

Contain a single policyIdentifier in the certificatePolicies extension that refers to the OID for the DCCKI Certificate Policy.

subjectAltName

Subject Alternative Name (SAN) shall be populated with the Fully Qualified Domain Name (FQDN) of the DCCKI Subscriber pertaining to the service for which the DCCKI Infrastructure Certificate will be used.

extendedKeyUsage

This shall be an extendedKeyUsage extension (as per section 4.2.1.12 of RFC 5280) with a value of id-kp-serverAuth and id-kp-clientAuth. This extension shall be marked as non-critical.

applicationPolicies

This shall be populated with the following policy identifies, Server Authentication and Client Authentication. This extension shall be marked as non-critical

cRLDistributionPoint

URI string, which shall identify the URL of the EII DCCKICA CRL within the DCCKI Repository. This extension shall be marked as non-critical.

authorityInfoAccess

URI string, which shall identify where to access information and services for the EII DCCKICA within the DCCKI Repository. This extension will be marked as non-critical.

DCCKI Infrastructure Certificate DCCKI Certificate Profile for the purposes of establishing SAML assertions

Field Name	RFC 5759/5280 Type	Value	Reference
Version	Integer	V3	
serialNumber	Integer	calculated by CA	
signatureAlgorithm		rsa-with-SHA256	
Issuer	Name	CN=EII DCCKICA O=DCC C=UK	
notBefore	Time	Calculated by CA as time of issue	
notAfter	Time	Calculated by CA as not before + 3 years	
Subject	Name	CN=Party Signifier	
subjectPublicKeyInfo		RSA	
keyLength		2048 bits	
Extensions	Extensions	Critical and non-critical extensions	
authorityKeyIdentifier	KeyIdentifier	Calculated by CA	

subjectKeyIdentifier	KeyIdentifier	Calculated by CA	
keyUsage		digitalSignature	
certificatePolicies		1.2.826.0.1.8641679.1.2.1.11	
cRLDistributionPoint	http location	[1] http://dcckirepo.prof.dsp.dccinterface.co.uk/revocationlists/download/EIIDCCKICA00.crt	
authorityInfoAccess	http location	[1] http://dcckirepo.prod.dsp.dccinterface.co.uk/certificatesearch/downloadcert/EIIDCCKICA00.crt	

Interpretation

Version

The version of the X.509 DCCKI Infrastructure Certificate. DCCKI Infrastructure Certificates shall identify themselves as version 3.

serialNumber

DCCKI Infrastructure Certificate serial number, a positive integer of no more than 20 octets. The Serial Number identifies the DCCKI Infrastructure Certificate, and shall be created by the Issuing EII DCCKICA that signs the DCCKI Infrastructure Certificate. The Serial Number shall be unique in the scope of DCCKI Infrastructure Certificates signed by the Issuing EII DCCKICA.

signatureAlgorithm

The identity of the signature algorithm used to sign the DCCKI Infrastructure Certificate. The field shall be rsa-with-SHA256 as defined in NIST FIPS 180-4.

Issuer

The name of the signer of the DCCKI Infrastructure Certificate. This will consist of the Country (C), Organisation Name (O) which will be DCC and a Common Name (CN) which will be EII DCCKICA (as defined in the EII DCCKICA Certificate certificate profile).

Validity

The time period over which the EII DCCKICA expects the DCCKI Infrastructure Certificate to be valid. The validity period is the period of time from notBefore through notAfter, inclusive.

All times shall be stated in the Universal Coordinated Time (UTC) time zone. Time up to and including 23:59:59 December 31, 2049 UTC shall be encoded as UTCTime as YYMMDDHHmmssZ.

Times later than 23:59:59 December 31, 2049 UTC shall be encoded as GeneralizedTime as YYYYMMDDHHmmssZ.

notBefore

The earliest time a DCCKI Infrastructure Certificate may be used. This shall be the time the DCCKI Infrastructure Certificate is created.

notAfter

The latest time a DCCKI Infrastructure Certificate is expected to be used. The value in a notAfter field shall be treated as specified in RFC 5280.

Subject

The formatting of this field shall contain a unique X.500 Distinguished Name (DN). This shall consist of a Common Name (CN) shall be populated with the Party Signifier of the DCCKI Subscriber.

subjectPublicKeyInfo

The Key Algorithm shall be RSA as defined in NIST FIPS 186-4.

keyLength

The Key length shall be RSA 2048 bits.

Extensions

DCCKI Infrastructure Certificates MUST contain the extensions described below. They SHOULD NOT contain any additional extensions:

- authorityKeyIdentifier.
- subjectKeyIdentifier
- keyUsage: critical
- certificatePolicies: non critical
- cRLDistributionPoint
- authorityInfoAccess

authorityKeyIdentifier

A key identifier calculated using method 2 of section 4.2.1.2 of RFC 5280.

subjectKeyIdentifier

Calculated using method 2 of section 4.2.1.2 of RFC 5280.

keyUsage

As per RFC 5280 section 4.2.1.3 with a value of digitalSignature.

certificatePolicies

Contain a single policyIdentifier in the certificatePolicies extension that refers to the OID for the DCCKI Certificate Policy.

cRLDistributionPoint

URI string, which shall identify the URL of the EII DCCKICA CRL within the DCCKI Repository. This extension shall be marked as non-critical.

authorityInfoAccess

URI string, which shall identify where to access information and services for the EII DCCKICA within the DCCKI Repository. This extension will be marked as non-critical.

Personnel Authentication Certificate DCCKI Certificate Profile (ordinary users)

Field Name	RFC 5759/5280 Type	Value	Reference
Version	Integer	V3	
serialNumber	Integer	calculated by CA	
signatureAlgorithm		rsa-with-SHA256	
Issuer	Name	CN= UI DCCKICA, O=DCC, C=UK	
notBefore	Time	Calculated by CA as time of issue	
notAfter	Time	Calculated by CA as not before + 3 years	

Subject	Name	CN = < Username>
		CN – UI DCCKICA
		O = DCC
		C = UK	

subjectPublicKeyInfo		RSA	
keyLength		2048 bits	

Extensions	Extensions	Critical and non-critical extensions	
authority Key Identifier	KeyIdentifier	Calculated by CA	
subject Key Identifier	KeyIdentifier	Calculated by CA	
keyUsage		digitalSignature	
certificatePolicies		1.2.826.0.1.8641679.1.2.1.11	
subjectAltName		Other Name =<username>	
extendedKeyUsage		Client Authentication (1.3.6.1.5.5.7.3.2)	

cRLDistributionPoint		[1] CRL Distribution Point Distribution Point Name:
		Full Name:
		Directory Address:
		CN=CRL1
		CN= UI DCCKICA
		O=DCC
		C=UK	

authorityInfoAccess	ldap location	[1]Authority Info Access Access Method=Certification Authority Issuer (1.2.6.1.5.5.7.48.2)
		Directory Address: CN=UI DCCKICA
		O=DCC
		C=UK	

Interpretation

Version

The version of the X.509 Personnel Authentication Certificate. Personnel Authentication Certificates shall identify themselves as version 3.

serialNumber

Personnel Authentication Certificate serial number, a positive integer of no more than 20 octets. The Serial Number identifies the Personnel Authentication Certificate, and shall be created by the Issuing UI DCCKICA that signs the Personnel Authentication Certificate. The Serial Number shall be unique in the scope of Personnel Authentication Certificates signed by the Issuing UI DCCKICA.

signatureAlgorithm

The identity of the signature algorithm used to sign the Personnel Authentication Certificate. The field shall be rsa-with-SHA256 as defined in NIST FIPS 180-4.

Issuer

The name of the signer of the Personnel Authentication Certificate. This will consist of the Country (C), Organisation Name (O) which will be DCC and a Common Name (CN) which will be UI DCCKICA (as defined in the UI DCCKICA Certificate certificate profile).

Validity

The time period over which the UI DCCKICA expects the Personnel Authentication Certificate to be valid. The validity period is the period of time from notBefore through notAfter, inclusive.

All times shall be stated in the Universal Coordinated Time (UTC) time zone. Time up to and including 23:59:59 December 31, 2049 UTC shall be encoded as UTCTime as YYMMDDHHmmssZ.

Times later than 23:59:59 December 31, 2049 UTC shall be encoded as GeneralizedTime as YYYYMMDDHHmmssZ.

notBefore

The earliest time a Personnel Authentication Certificate may be used. This shall be the time the Personnel Authentication Certificate is created.

notAfter

The latest time a Personnel Authentication Certificate is expected to be used. The value in a notAfter field shall be treated as specified in RFC 5280.

Subject

The formatting of this field shall contain a unique X.500 Distinguished Name (DN). This shall consist of a Common Name (CN) which shall uniquely identify the DCCKI Eligible Subscriber who is the subject of this account and must be consistent with the information held in the User Personnel's SSI account.

subjectKeyPublicInfo

The Public Key algorithm shall be RSA as defined in NIST FIPS 186-4.

keyLength

The Key length shall be RSA 2048 bits.

Extensions

Personnel Authentication Certificates MUST contain the extensions described below. They SHOULD NOT contain any additional extensions:

- authorityKeyIdentifier
- subjectKeyIdentifier
- keyUsage: critical
- certificatePolicies: non critical
- subjectAltName: non-critical
- extendedKeyUsage: non critical
- cRLDistributionPoint
- AuthorityInformationAccess

authorityKeyIdentifier

This shall be in the form [0] KeyIdentifier. This shall be generated using method (2) of section 4.2.1.2 of RFC 5280. This extension shall be marked as non-critical.

subjectKeyIdentifier

Calculated using method 2 of section 4.2.1.2 of RFC 5280.

keyUsage

As per RFC 5280 section 4.2.1.3 with a value of digitalSignature. This extension shall be marked as critical.

certificatePolicies

Contain a single policyIdentifier in the certificatePolicies extension that refers to the OID for the DCCKI Certificate Policy.

subjectAltName

The Personnel Authentication Certificate shall contain a single GeneralName of type OtherName. The OtherName shall be the SSI username of the User Personnel of the DCCKI Eligible Subscriber.

extendedKeyUsage

This shall be an extendedKeyUsage extension (as per RFC 5280 section 4.2.1.12) with a value id-kp-clientAuth. This extension shall be marked as non-critical.

cRLDistributionPoint

This shall identify the directory address of the UI DCCKICA CRL. This extension shall be marked as non-critical.

AuthorityInformationAccess

This shall identify the directory address of the UK DCCKICA Certificate. This extension shall be marked as non-critical.

Personnel Authentication Certificate DCCKI Certificate Profile (Administration Users)

Field Name	RFC 5759/5280 Type	Value	Reference
Version	Integer	V3	
serialNumber	Integer	calculated by CA	
signatureAlgorithm		rsa-with-SHA256	
Issuer	Name	CN= UI DCCKICA, O=DCC, C=UK	
notBefore	Time	Calculated by CA as time of issue	
notAfter	Time	Calculated by CA as not before + 3 years	
Subject	Name	CN = <Name>	

		CN= UI DCCKICA
		O=DCC
		C=UK	

subjectPublicKeyInfo		RSA	
keyLength		2048 bits	
Extensions	Extensions	Critical and non-critical extensions	
authority Key Identifier	KeyIdentifier	Calculated by CA	
subject Key Identifier	KeyIdentifier	Calculated by CA	
keyUsage		digitalSignature	

certificatePolicies		[1] 2.16.840.1.101.3.2.1.3.13 (PIV Authentication Key OID) [2] 1.2.826.0.1.8641679.1.2.1.11 (DCCKI CP OID)	
subjectAltName		Other Name =<username> Other Name=<UUID>	
extendedKeyUsage		Client Authentication (1.3.6.1.5.5.7.3.2) Smart Card Logon (1.3.6.1.4.1.311.20.2.2)	

cRLDistributionPoint		[1]CRL Distribution Point
		Distribution Point Name:
		Full Name:
		Directory Address:
		CN=CRL1
		CN= UI DCCKICA
		O=DCC
		C=UK
			cRLDistributionPoint

authorityInfoAccess	ldap location	[1]Authority Info Access Access Method=Certification Authority Issuer (1.2.6.1.5.5.7.48.2)
		Alternative Name:
		Directory Address:
		CN=UI DCCKICA
		O=DCC
		C=UK	

2.16.840.1.101.3.2.1.3.6.9.1		(01 01 00) ((PIV Authenticationidentifier)	PIV authentication OID

Interpretation

Version

The version of the X.509 Personnel Authentication Certificate. Personnel Authentication Certificates shall identify themselves as version 3.

serialNumber

Personnel Authentication Certificate serial number, a positive integer of no more than 20 octets. The Serial Number identifies the Personnel Authentication Certificate, and shall be created by the Issuing UI DCCKICA that signs the Personnel Authentication Certificate. The Serial Number shall be unique in the scope of Personnel Authentication Certificates signed by the Issuing UI DCCKICA.

signatureAlgorithm

The identity of the signature algorithm used to sign the Personnel Authentication Certificate. The field shall be rsa-with-SHA256 as defined in NIST FIPS 180-4.

Issuer

The name of the signer of the Personnel Authentication Certificate. This will consist of the Country (C), Organisation Name (O) which will be DCC and a Common Name (CN) which will be UI DCCKICA (as defined in the UI DCCKICA Certificate certificate profile).

Validity

The time period over which the UI DCCKICA expects the Personnel Authentication Certificate to be valid. The validity period is the period of time from notBefore through notAfter, inclusive.

All times shall be stated in the Universal Coordinated Time (UTC) time zone. Time up to and including 23:59:59 December 31, 2049 UTC shall be encoded as UTCTime as YYMMDDHHmmssZ.

Times later than 23:59:59 December 31, 2049 UTC shall be encoded as GeneralizedTime as YYYYMMDDHHmmssZ.

notBefore

The earliest time a Personnel Authentication Certificate may be used. This shall be the time the Personnel Authentication Certificate is created.

notAfter

The latest time a Personnel Authentication Certificate is expected to be used. The value in a notAfter field shall be treated as specified in RFC 5280.

Subject

The formatting of this field shall contain a unique X.500 Distinguished Name (DN). This shall consist of a Common Name (CN) which shall be the First and Last name and FQDN to identify the users account of the Eligible DCCKI Subscribe this shall be consistent with the information held in the Administration User's SSI account.

subjectKeyPublicInfo

The Public Key algorithm shall be RSA as defined in NIST FIPS 186-4.

keyLength

The Key length shall be RSA 2048 bits.

Extensions

Personnel Authentication Certificates MUST contain the extensions described below. They SHOULD NOT contain any additional extensions:

- authorityKeyIdentifier
- subjectKeyIdentifier
- keyUsage: critical
- certificatePolicies: non-critical
- subjectAltName: non-critical
- extendedKeyUsage: non-critical
- cRLDistributionPoint
- AuthorityInformationAccess
- 2.16.840.1.101.3.6.9.1 PIV Authentication Identifier

authorityKeyIdentifier

This shall be in the form [0] KeyIdentifier. This shall be generated using method (2) of section 4.2.1.2 of RFC 5280. This extension shall be marked as non-critical.

subjectKeyIdentifier

Calculated using method 2 of section 4.2.1.2 of RFC 5280.

keyUsage

As per RFC 5280 section 4.2.1.3 with a value of digitalSignature. This extension shall be marked as critical (as per RFC 5280 section 4.2.1.3).

certificatePolicies

Contain a policyIdentifier in the certificatePolicies extension that refers to the OID for the DCCKI Certificate Policy and a policyIdentifier with PIV Authentication Key OID.

subjectAltName

The Personnel Authentication Certificate shall contain 2 GeneralName entries of type OtherName. The first OtherName shall be consistent with the SSI username of the Administration User. The second OtherName entry shall contain a UUID which uniquely identifies the DCCKI Eligible Subscriber.

extendedKeyUsage

This shall be an extendedKeyUsage extension (as per RFC 5280 section 4.2.1.12) with a value id-kp-clientAuth and a value of "Smart Card Logon". This extension shall be marked as non-critical.

cRLDistributionPoint

This shall identify the directory address of the UI DCCKICA CRL. This extension shall be marked as non-critical.

AuthorityInformationAccess

This shall identify the directory address of the UI DCCKICA Certificate. This extension shall be marked as non-critical.

2.16.840.1.101.3.6.9.1 PIV Authentication Identifier

Personal Identity Verification (PIV) identifier included in all Personnel Authentication Certificate issued to Administration User.

EII DCCKICA Certificate DCCKI Certificate Profile

Field Name	RFC 5759/5280 Type	Value	Reference
Version	Integer	V3	
serialNumber	Integer	calculated by CA	
signatureAlgorithm		rsa-with-SHA256	
Issuer	Name	CN= Root DCCKICA, O=DCC, C=UK	
notBefore	Time	Calculated by CA as time of issue	
notAfter	Time	Calculated by CA as not before + 10 years	
Subject	Name	CN= EII DCCKICA, O=DCC, C=UK	
subjectKeyPublicInfo		RSA	
keyLength		2048 bits	
Extensions	Extensions	Critical and non-critical extensions	
authorityKeyIdentifier	KeyIdentifier	Calculated by CA	

subjectKeyIdentifier	KeyIdentifier	Calculated by CA	
keyUsage		Certificate Signing, Off-line CRL Signing CRL Signing	
certificatePolicies		1.2.826.0.1.8641679.1.2.1.11;	
basicConstraints		CA=True, path Length=0	

cRLDistributionPoint	http location	[1] CRL Distribution Point
		URL=http://dcckirepo.prod.dsp.dccinterface.co.uk/revocationlists/download/RootDCCKICA-00.crl >
		[2] CRL Distribution Point
		Distribution Point Name:
		Full Name:
		Directory Address:
		CN=CRL1
		CN= Root DCCKICA
		O=DCC
		C=UK	

authorityInfoAccess	http location	[1] Authority Info Access Alternative Name: URL=http://dcckirepo.prod.dsp.dccinterface.co.uk/certificatesearch/downloadcert/RootDCCKICA-00.crt	

Interpretation

Version

The version of the X.509 EII DCCKICA Certificate. EII DCCKICA Certificates shall identify themselves as version 3.

serialNumber

EII DCCKICA Certificate serial number, a positive integer of no more than 20 octets. The Serial Number identifies the EII DCCKICA Certificate, and shall be created by the Root DCCKICA that signs the EII DCCKICA Certificate. The Serial Number shall be unique in the scope of DCCKICA Certificates signed by the Root DCCKICA.

signatureAlgorithm

The identity of the signature algorithm used to sign the EII DCCKICA Certificate. The field shall be rsa-with-SHA256 as defined in NIST FIPS 180-4.

Issuer

The name of the signer of the EII DCCKICA Certificate. This will consist of the Country (C), Organisation Name (O) which will be DCC and a Common Name (CN) which will be Root DCCKICA (as defined in the Root DCCKICA Certificate profile).

Validity

The time period over which the Root DCCKICA expects the EII DCCKICA Certificate to be valid. The validity period is the period of time from notBefore through notAfter, inclusive.

All times shall be stated in the Universal Coordinated Time (UTC) time zone. Time up to and including 23:59:59 December 31, 2049 UTC shall be encoded as UTCTime as YYMMDDHHmmssZ.

Times later than 23:59:59 December 31, 2049 UTC shall be encoded as GeneralizedTime as YYYYMMDDHHmmssZ.

notBefore

The earliest time an EII DCCKICA Certificate may be used. This shall be the time the EII DCCKICA Certificate is created.

notAfter

The latest time an EII DCCKICA Certificate is expected to be used. The value in a notAfter field shall be treated as specified in RFC 5280.

Subject

The formatting of this field shall contain a unique X.500 Distinguished Name (DN). This shall consist of the Country (C), the Organisation Name (O) which will be DCC and a Common Name (CN) which will be EII DCCKICA.

subjectKeyPublicInfo.

The Public Key algorithm shall be RSA as defined in NIST FIPS 186-4.

keyLength

The keyLength shall be RSA 2048 bits.

Extensions

EII DCCKICA Certificates MUST contain the extensions described below. They SHOULD NOT contain any additional extensions:

- authorityKeyIdentifier.
- subjectKeyIdentifier
- keyUsage: critical

- certificatePolicies: non critical
- basicConstraints: critical.
- cRLDistributionPoint
- authorityInfoAccess

authorityKeyIdentifier

A key identifier calculated using method 2 of section 4.2.1.2 of RFC 5280.

subjectKeyIdentifier

Calculated using method 2 of section 4.2.1.2 of RFC 5280.

keyUsage

The EII DCCKICA Certificate shall have a keyUsage extension (as per section 4.2.1.3 of RFC 5280) with a value of Certificate Signing, Off-line CRL Signing and CRL Signing. This extension shall be marked as critical (as per RFC 5280 section 4.2.1.3).

certificatePolicies

The EII DCCKICA Certificate shall contain at least one policyIdentifier in the certificatePolicies extension that refers to the OID for the DCCKI Certificate Policy.

basicConstraints

The basicConstraints extension shall have the values cA=True, and pathLen=0. This extension shall be marked as critical.

cRLDistributionPoint

URI string, which shall identify the URL of the DCCK ARL within the DCCKI Repository. This extension shall be marked as non-critical.

authorityInfoAccess

URI string, which shall identify where to access information and services for the Root DCCKICA within the DCCKI Repository. This extension will be marked as non-critical.

UI DCCKICA Certificate DCCKI Certificate Profile

Field Name	RFC 5759/5280 Type	Value	Reference
Version	Integer	V3	
serialNumber	Integer	calculated by CA	
signatureAlgorithm		rsa-with-SHA256	

Issuer	Name	CN= Root DCCKICA, O=DCC, C=UK	
notBefore	Time	Calculated by CA as time of issue	
notAfter	Time	Calculated by CA as not before + 10 years	
Subject	Name	CN=UI DCCKICA, O=DCC, C=UK	
subjectPublicKeyInfo		RSA	
keyLength		2048 bits	
Extensions	Extensions	Critical and non-critical extensions	
authorityKeyIdentifier	KeyIdentifier	Calculated by CA	
subjectKeyIdentifier	KeyIdentifier	Calculated by CA	
keyUsage		Certificate Signing Off-line CRL Signing CRL Signing	
certificatePolicies		1.2.826.0.1.8641679.1.2.1.11;	
basicConstraints		CA=True, path Length=0	

cRLDistributionPoint	http location	[1] CRL Distribution Point Distribution Point Name:
		Full Name:
		Directory Address:
		CN=CRL1
		CN= Root DCCKICA
		O=DCC
		C=UK
			cRLDistributionPoint

Interpretation

Version

The version of the X.509 UI DCCKICA Certificate. UI DCCKICA Certificates shall identify themselves as version 3.

serialNumber

UI DCCKICA Certificate serial number, a positive integer of no more than 20 octets. The Serial Number identifies the UI DCCKICA Certificate, and shall be created by the Root DCCKICA that signs the UI DCCKICA Certificate. The Serial Number shall be unique in the scope of DCCKICA Certificates signed by the Root DCCKICA.

signatureAlgorithm

The identity of the signature algorithm used to sign the UI DCCKICA Certificate. The field shall be rsa-with-SHA256 as defined in NIST FIPS 180-4.

Issuer

The name of the signer of the UI DCCKICA Certificate. This will consist of the Country (C), Organisation Name (O) which will be DCC and a Common Name (CN) which will be Root DCCKICA (as defined in the Root DCCKICA Certificate profile).

Validity

The time period over which the Root DCCKICA expects the UI DCCKICA Certificate to be valid. The validity period is the period of time from notBefore through notAfter, inclusive.

All times shall be stated in the Universal Coordinated Time (UTC) time zone. Time up to and including 23:59:59 December 31, 2049 UTC shall be encoded as UTCTime as YYMMDDHHmmssZ.

Times later than 23:59:59 December 31, 2049 UTC shall be encoded as GeneralizedTime as YYYYMMDDHHmmssZ.

notBefore

The earliest time a UI DCCKICA Certificate may be used. This shall be the time the UI DCCKICA Certificate is created.

notAfter

The latest time a UI DCCKICA Certificate is expected to be used. The value in a notAfter field shall be treated as specified in RFC 5280.

Subject

The formatting of this field shall contain a unique X.500 Distinguished Name (DN). This shall consist of the Country (C), the Organisation Name (O) which will be DCC and a Common Name (CN) which will be UI DCCKICA.

subjectPublicKeyInfo

The Public Key algorithm shall be RSA as defined in NIST FIPS 186-4.

keyLength

The Key length shall be RSA 2048 bits.

Extensions

UI DCCKICA Certificates MUST contain the extensions described below. They SHOULD NOT contain any additional extensions:

- authorityKeyIdentifier.
- subjectKeyIdentifier
- keyUsage: critical
- certificatePolicies: non critical
- basicConstraints: critical.
- cRLDistributionPoint

authorityKeyIdentifier

A key identifier calculated using method 2 of section 4.2.1.2 of RFC 5280.

subjectKeyIdentifier

Calculated using method 2 of section 4.2.1.2 of RFC 5280.

keyUsage

The UI DCCKICA Certificate shall have a keyUsage extension (as per section 4.2.1.3 of RFC 5280) with a value of Certificate Signing, Off-line CRL Signing and CRL Signing. This extension shall be marked as critical (as per section 4.2.1.3 of RFC 5280).

certificatePolicies

The UI DCCKICA Certificate shall contain at least one policyIdentifier in the certificatePolicies extension that refers to the OID for the DCCKI Certificate Policy.

basicConstraints

The basicConstraints extension shall have the values cA=True, and pathLen=0. This extension shall be marked as critical.

cRLDistributionPoint

LDAP string, which shall refer to the Root DCCKICA ARL. This extension shall be marked as non-critical.

Root DCCKICA Certificate DCCKI Certificate Profile

Field Name	RFC 5759/5280 Type	Value	Reference
Version	Integer	V3	

serialNumber	Integer	calculated by CA	
signatureAlgorithm	AlgortithmIdentifier	rsa-with-SHA256	
Issuer	Name	CN= Root DCCKICA, O=DCC, C=UK	
notBefore	Time	Calculated by CA as time of issue	
notAfter	Time	Calculated by CA as not before + 20 years	
Subject	Name	CN=Root DCCKICA, O=DCC, C=UK	
subjectPublicKeyInfo		RSA	
keyLength		4096 bits	
Extensions	Extensions	Critical and non-critical extensions	
authorityKeyIdentifier	KeyIdentifier	Calculated by CA	
subjectKeyIdentifier	KeyIdentifier	Calculated by CA	
keyUsage		Certificate Signing, Off-line CRL Signing and CRL Signing	
certificatePolicies		anyPolicy	
basicConstraints		CA=True, path Length= None	

Interpretation

These certificates are the root of trust for the DCCKI.

Version

The version of the X.509 Root DCCKICA Certificate. Valid Root DCCKICA Certificates shall identify themselves as version 3.

Serial Number

Root DCCKICA Certificate serial number, a positive integer of no more than 20 octets. The Serial Number identifies the Root DCCKICA Certificate, and shall be created by the Root DCCKICA that signs the Root DCCKICA Certificate (self-signed by the Root DCCKICA). The Serial Number shall be unique in the scope of DCCKICA Certificate signed by the Root DCCKICA.

signatureAlgorithm

The identity of the signature algorithm used to sign the Root DCCKICA Certificate. The field shall be rsa-with-SHA256 as defined in NIST FIPS 180-4.

Issuer

The name of the signer of the Root DCCKICA Certificate. This will consist of the Country (C), Organisation Name (O) which will be DCC and a Common Name (CN) which will be Root DCCKICA which will be the same as the Subject Name as it is self-signed by the Root DCCKICA.

Validity

The time period over which the Root DCCKICA expects the Root DCCKICA Certificate to be valid. The validity period is the period of time from notBefore through notAfter, inclusive.

All times shall be stated in the Universal Coordinated Time (UTC) time zone. Times up to and including 23:59:59 December 31, 2049 UTC shall be encoded as UTCTime as YYMMDDHHmmssZ.

Times later than 23:59:59 December 31, 2049 UTC shall be encoded as GeneralizedTime as YYYYMMDDHHmmssZ

notBefore

The earliest time a Root DCCKICA Certificate may be used. This shall be the time the Root DCCKICA Certificate is created.

notAfter

The latest time a Root DCCKICA Certificate is expected to be used. The value in a notAfter field shall be treated as specified in RFC 5280.

Subject

The formatting of this field shall contain a unique X.500 Distinguished Name (DN). This shall consist of the Country (C), the Organisation Name (O) which will be DCC and a Common Name (CN) which will be Root DCCKICA.

subjectPublicKeyInfo.

The Public Key algorithm shall be RSA as defined in NIST FIPS 180-6.

keyLength

The keyLength shall be RSA 4096 bits.

Extensions

Root DCCKICA Certificate MUST contain the extensions described below. They SHOULD NOT contain any additional extensions:

- authorityKeyIdentifier.
- subjectKeyIdentifier
- keyUsage: critical
- certificatePolicies: non critical
- basicConstraints: critical.

authorityKeyIdentifier

A keyIdentifier calculated using method 2 of section 4.2.1.2 of RFC 5280.

subjectKeyIdentifier

Calculated using method 2 of section 4.2.1.2 of RFC 5280.

keyUsage

The Root DCCKICA Certificate shall have a keyUsage extension (as per RFC 5280 section 4.2.1.3) with a value of Certificate Signing, Off-line CRL Signing and CRL Signing. This extension shall be marked as critical (as per RFC 5280 section 4.2.1.3).

certificatePolicies

The RootDCCKICA Certificate shall contain only one policyIdentifier which shall be any Policy.

basicConstraints

The basicConstraints extension shall have the values cA=True, and pathLen absent (unlimited). This extension shall be marked as critical.

Version: T3.0

Appendix T

DCCKI Interface Design Specification

Contents

1. INTRODUCTION

Document Purpose

1.1 Pursuant to Section L13.13 of the Code (DCCKI Interface Design Specification), this document is the DCCKI Interface Design Specification (DCCKI IDS).

2. DCCKI SERVICE INTERFACE

Submission of DCCKI Certificate Signing Requests and Issuance of DCCKI Infrastructure Certificates

2.1 In order to request Issuance of a DCCKI Infrastructure Certificate, a Party or RDP that is a DCCKI Eligible Subscriber shall follow the processes defined in the DCCKI RAPP.

2.2 The DCC shall ensure that all DCCKI Certificate Signing Requests are required to be formatted in accordance with the PKCS#10 standard as set out in the DCCKI RAPP. The structure of a DCCKI Certificate Signing Request is defined in section 3 of this DCCKI IDS.

2.3 No further provision is made in this document in relation to requesting and obtaining DCCKI Infrastructure Certificates.

Submission of Personnel Authentication Certificate Applications and Issuance of Personnel Authentication Certificates

2.4 Prior to submitting an initial Personnel Authentication Certificate Application, (but not for any subsequent application), a Party that is a DCCKI Eligible Subscriber in respect of Personnel Authentication Certificates shall submit an Administration User Credentials Request via the approved mechanisms set out in the DCCKI RAPP section 3.19.

2.5 The DCC shall make a Personnel Credentials Interface accessible via the Self Service Interface for the purpose of accessing DCCKI Services in order to obtain a Personnel Authentication Certificate. The DCC shall ensure that:

(a) the Personnel Credentials Interface uses the HTTPS protocol;

(b) the Personnel Credentials Interface uses Java 7, update 6 (or greater);

(c) the Personnel Credentials Interface supports JavaScript, CSS and images;

(d) initial access to the Personnel Credentials Interface will be authorised through use of username and single use password, the provision of which shall be detailed in the DCCKI RAPP and shall be secured by server side authentication using TLS;

(e) subsequent access to the Personnel Credentials Interface is secured by mutual authentication using TLS between the supported browser being used by the DCCKI Eligible Subscriber and the Personnel Credentials Interface;

(f) DCCKI Certificates are used for the TLS authentication and shall support the following cipher suites:

i. ECDHE-RSA-AES256-GCM-SHA384

ii. ECDHE-RSA-AES128-GCM-SHA256

iii. ECDHE-RSA-AES256-SHA384

iv. ECDHE-RSA-AES128-SHA256;

(g) access to the Personnel Credentials Interface is denied without a valid credential for Authentication; and

(h) User Personnel are provided with the means to view and update their password and user account information as set out in the Self Service Interface Access Control Specification.

Issuance of Personnel Authentication Certificates to Administration Users

Initial Issuance of a Personnel Authentication Certificate to Administration Users

2.6 In order to obtain an initial Personnel Authentication Certificate, an Administration User shall log onto the Personnel Credentials Interface via the Self Service Interface using the supplied username, and single use password as provided in accordance with the DCCKI RAPP.

2.7 Upon initial login, the SSI Administration User shall be required to:

(a) change the password for the user account from that provided; and

(b) provide answers to security questions that will subsequently be used to confirm the identity of that Administration User if their password is forgotten, their Personnel Authentication Certificate has expired or the Smart Card Token provided to that Administration User is lost or stolen.

2.8 On successful change of the user account password, the Administration User shall be able to request initialisation of the Smart Card Token which will result in a Personnel Authentication Certificate Application.

2.9 In order to initialise the Smart Card Token, the Administration User shall:

(a) connect the Smart Card Token to the system that the Administration User is using to access the Personnel Credentials Interface. The system shall be configured in accordance with sections 2.5 (b) and (c) of this DCCKI IDS; and

(b) request initialisation of the Smart Card Token by following the instructions displayed on the Personnel Credentials Interface.

2.10 Following a successful request for initialisation of the Smart Card Token the DCC shall ensure that, where the Smart Card Token generates a Personnel Authentication Certificate Application, this shall automatically be submitted to the UI DCCKICA.

2.11 The Administration User shall be notified via the Personnel Credentials Interface as soon as reasonably practicable of the Issuance of a Personnel Authentication Certificate for that Administration User.

Subsequent Issuance of a Personnel Authentication Certificate to Administration Users

2.12 Prior to the expiry of a Personnel Authentication Certificate Issued to an Administration User, that Administration User may:

(a) log onto the Personnel Credentials Interface via the Self Service Interface, using their Smart Card Token, username and password; and

(b) reinitialise the Smart Card Token by following the steps set out in section 2.9 of this DCCKI IDS, which will result in the Issuance of a new Personnel Authentication Certificate.

2.13 In the event that a Personnel Authentication Certificate Issued to an Administration User has expired prior to their obtaining a new Personnel Authentication Certificate, that Administration User may:

(a) log onto the Personnel Credentials Interface via the Self Service Interface and obtain a new Personnel Authentication Certificate by:

(i) using their Administration User username and password; and

(ii) providing answers to the security questions as selected when obtaining their initial Personnel Authentication Certificate; and

(b) reinitialise the Smart Card Token by following the steps outlined in section 2.9 above which will result in the Issuance of a new Personnel Authentication Certificate.

2.14 In the event that the Smart Card Token is lost or stolen, an Administration User may:

(a) obtain a new Smart Card Token from their DCCKI ARO in accordance with the DCCKI Code of Connection;

(b) log onto the Personnel Credentials Interface via the Self Service Interface:

(i) using the Administration User's username and password; and

(ii) providing answers to the security questions as selected when obtaining their initial Personnel Authentication Certificate; and

(c) initialise the Smart Card Token by following the steps outlined in section 2.9 of this DCCKI IDS which will result in the Issuance of a new Personnel Authentication Certificate.

Issuance of Personnel Authentication Certificates to other User Personnel

Initial Issuance of a Personnel Authentication Certificate to other User Personnel

2.15 The initial Issuance of a Personnel Authentication Certificate to a User Personnel shall be via the Personnel Credentials Interface following the creation of an account for that User Personnel by an Administration User.

2.16 In order to provide Authentication credentials to User Personnel, (which shall comprise a single use password and a username) an Administration User may:

(a) log onto the Self Service Interface using their Smart Card Token, username and password in accordance with the Self Service Interface Access Control Specification and Self Service Interface Code of Connection;

(b) create additional user accounts for other User Personnel; and

(c) provide details to those User Personnel including a username and single use password that allows them to log onto the Personnel Credentials Interface via the Self Service Interface.

2.17 In order to obtain an initial Personnel Authentication Certificate, User Personnel of a DCCKI Eligible Subscriber, shall log onto the Personnel Credentials Interface via the Self Service Interface using the agreed username and single use password, as established by the relevant Administration User.

2.18 Upon first login, those User Personnel shall be required to:

(a) change the password for their account; and

(b) provide answers to security questions that will subsequently be used to confirm the identity of that individual if the password is forgotten, their Personnel Authentication Certificate has expired or their Personnel Authentication Certificate is destroyed or, no longer has access to their Personnel Authentication Certificate or Private Key associated with their Personnel Authentication Certificate.

2.19 Upon successful login, the User Personnel shall be able to submit a Personnel Authentication Certificate Application by following the instruction displayed on the Personnel Credentials Interface.

2.20 Following a Personnel Authentication Certificate Application request:

(a) the User Personnel shall be requested to create a password in accordance with the instruction displayed on the Personnel Credentials Interface, to protect the credentials to be generated by the DCCKICA and transferred to the User Personnel's browser;

(b) the DCCKI Eligible Subscriber shall ensure that the systems of its User Personnel are configured to allow the credentials to be transferred to the User Personnel's browser and in accordance with sections 2.5 (b) and (c) of this DCCKI IDS;

(c) the DCCKICA shall generate the credentials consisting of a Key Pair along with a Personnel Authentication Certificate that is specific to that User Personnel and the systems that User Personnel is using to access the Personnel Credentials Interface and shall make it available to the browser in the form of a PKCS#12 file protected using the password created by the User Personnel;

(d) the User Personnel shall unprotect the PKCS#12 file using the password created by that User Personnel; and

(e) the User Personnel shall download, verify and install the PKCS#12 file in a location accessible to a supported web browser, when requested by the Authentication Credentials Interface.

Subsequent Issuance of a Personnel Authentication Certificate to other User Personnel

2.21 Prior to the expiry of a Personnel Authentication Certificate assigned to a member of User Personnel, in order to obtain a new Personnel Authentication Certificate, that individual:

(a) may log onto the Personnel Credentials Interface via the Self Service Interface, using their existing Personnel Authentication Certificate, username and password; and

(b) follow the steps outlined in sections 2.19 and 2.20 of this DCCKI IDS.

2.22 In the event that their Personnel Authentication Certificate has expired prior to obtaining a new Personnel Authentication Certificate, a member of User Personnel may:

(a) Log onto the Personnel Credentials Interface via the Self Service Interface:

(i) using their username and password; and

(ii) provide answers to the security questions as selected when obtaining their initial Personnel Authentication Certificate; and

(b) follow the steps outlined in sections 2.19 and 2.20 of this DCCKI IDS.

3. DCCKI CERTIFICATE SIGNING REQUEST

Information to be contained within DCCKI Certificate Signing Requests

3.1 A DCCKI Certificate Signing Request in respect of a DCCKI Infrastructure Certificate for the purpose of signing SAML assertions to the DCC shall contain the information set out in the table immediately below:

Subject	Attributes	Values
Version		V3 (as per RFC 2986)
Subject	Common Name	<Party Signifier>

Subject Public Key Info	Public Key Algorithm	RSA
	Subject Public Key (2048 bits)	Public Key value
Key Usage	Criticality	True
	Key Usage	digitalSignature
Signature Algorithm		rsa-with-SHA256

3.2 A DCCKI Certificate Signing Request in respect of a DCCKI Infrastructure Certificate for the purpose of establishing TLS communications to the DCC shall contain the information set out in the table immediately below:

Subject	**Attributes**	**Values**
Version		V3 (as per RFC 2986)
Subject	Common Name	Fully Qualified Domain Name configured on the Policy Enforcement Point
	Organisation Identifier	Party Signifier or RDP Signifier
Subject Public Key Info	Public Key Algorithm	RSA
	Subject Public Key (2048 bits)	Public Key Value
Key Usage	Criticality	True
	Key Usage	digitalSignature keyEncipherment
Signature Algorithm		rsa-with-SHA256

3.3 A DCCKI Certificate Signing Request in respect of a DCCKI Infrastructure Certificate for the purpose of establishing FTPS communications to the DCC shall contain the information set out in the table immediately below:

Subject	**Attributes**	**Values**
Version		V3 (as per RFC 2986)
Subject	Common Name	Party Signifier or RDP Signifier
Subject Alt Name		<Fully Qualified Domain Name>

Subject Public Key Info	Public Key Algorithm	RSA
	Subject Public Key (2048 bits)	Public Key value

Key Usage	Criticality	True
	Key Usage	digitalSignature keyEncipherment

Signature Algorithm		rsa-with-SHA256

DCCKI Certificate Signing Request format

3.4 DCCKI Certificate Signing Request requests shall be formatted according to PKCS#10, Base64 encoded.

3.5 The standard format shall be ASN.1 DER, including one of the immediately following two styles of PEM header:

(a) -----BEGIN CERTIFICATE REQUEST----- and -----END CERTIFICATE REQUEST-----; or

(b) -----BEGIN NEW CERTIFICATE REQUEST----- and -----END NEW CERTIFICATE REQUEST-----

Acceptable DCCKI Certificate Signing Request variants

3.6 The DCC shall accept the following PKCS#10 variants:

(a) Base64 all in one line;

(b) Base64 with line breaks at 64 or 76 characters; and

(c) if line breaks are used the \n and \r\n are both acceptable.

Signing the DCCKI Certificate Signing Request using a Private Key associated with an Organisation Certificate

3.7 Following the creation of the DCCKI Certificate Signing Request in accordance with section 3.4 of this DCCKI IDS, the DCCKI Eligible Subscriber shall Digitally Sign the DCCKI Certificate Signing Request with a Private Key associated with an Organisation Certificate for which it is a Subscriber.

3.8 The DCCKI Eligible Subscriber shall ensure that the Digital Signature shall:

(a) use, as the digital signature technique, Elliptic Curve Digital Signature Algorithm (ECDSA) (as specified in Federal Information Processing Standards Publications (FIPS PUB) 186-4) in combination with the curve P- 256 (as specified in FIPS PUB 186-4 at section D.1.2.3) and SHA-256 as the Hash function;

(b) be applied to the entirety of the PKCS#10 file, including header and footer; and

(c) be converted to Base64 and appended to the footer within the PKCS#10 file itself with a preceding "," separator.

3.9 Prior to Digitally Signing the DCCKI Certificate Signing Request, the DCCKI Eligible Subscriber shall append to the footer of the PKCS#10 file, the Issuer which shall be URL encoded (as specified in the IETF RFC 1) and serial number of the Organisation Certificate with preceding "," separators.

Availability and Service Continuity

3.10 The DCC shall ensure that the DCCKI Service Interface is available, in accordance with Section L13.12 (the DCCKI Service Interface) of the Code.

3.11 The DCC shall notify Parties and RDPs in advance of any planned outages of the DCCKI Service Interface.

ANNEX A

DEFINITIONS

In this document, except where the context otherwise requires:

- expressions defined in Section A of the Code (Definitions and Interpretation) have the same meaning as is set out in that section; and
- any expressions not defined here or in Section A of the Code have the meaning given to them in the DCCKI Certificate Policy, the DCCKI Registration Authority Policies and Procedures or the Self Service Interface Access Control Specification.

Issuer	The name of the signer of the DCCKI Infrastructure Certificate as described in the DCCKI Certificate Policy.

Version: U2.0

Appendix U

DCCKI Repository Interface Design Specification

1. INTRODUCTION

Document Purpose

1.1 This DCCKI Repository Interface Design Specification is the document required by Section L13.27 of the SEC.

2. DCCKI REPOSITORY INTERFACE

2.1 Pursuant to Section L13.27 (DCCKI Repository Interface Design Specification) of the Code, the DCCKI Repository Interface is a web portal interface designed to allow communications with the DCC for the purposes of the DCCKI Repository Service.

2.2 The DCCKI Repository shall only be accessible via a DCC Gateway Connection.

2.3 The DCC shall make the DCCKI Repository Interface available to:

(a) all Parties which are Users; and

(b) RDPs,

using a DCC Gateway Connection via anonymous access (that is, without requiring authentication).

2.4 A Party which is a User or an RDP shall access the DCCKI Repository via a supported web browser.

2.5 The DCC shall ensure that the DCCKI Repository Interface:

(a) uses the HTTP protocol;

(b) supports JavaScript, Cascading Style Sheets and images; and

(c) is provided at Uniform Resource Locators in accordance with the DCCKI Repository Code of Connection.

2.6 A Party or RDP shall:

(a) use the DCCKI Repository Interface to access the DCCKI Repository, in order to obtain the information listed in Section L13.17 (The DCCKI Repository) of the Code; and

(b) in accessing the DCCKI Repository, ensure that their supported web browser has JavaScript enabled.

Availability and Service Continuity

2.7 The DCC shall ensure that the DCCKI Repository Interface is available in accordance with Section L13.25 (the DCCKI Repository Interface) of the Code.

2.8 The DCC shall notify Parties and RDPs in advance of any planned outages of the DCCKI Repository Interface.

ANNEX A

DEFINITIONS

In this document, except where the context otherwise requires:

- expressions defined in Section A of the Code (Definitions and Interpretation) have the same meaning as is set out in that section; and

- any expressions not defined here or in Section A of the Code have the meaning given to them in the DCCKI Certificate Policy, the DCCKI Registration Authority Policies and Procedures or the Self Service Interface Access Control Specification.

Version: V2.0

Appendix V

DCCKI Code of Connection and DCCKI Repository Code of Connection

1. INTRODUCTION

1.1 This DCCKI Code of Connection and DCCKI Repository Code of Connection is the document required by Section L13.14 and Section L13.28 of the Code.

2. GENERAL OBLIGATIONS

2.1 Each DCCKI Authorised Subscriber may connect to the DCCKI Service Interface or the DCCKI Repository Interface only via a DCC Gateway Connection and for the purposes set out in the Code and this DCCKI Code of Connection.

2.2 The DCC shall ensure that the any URL and IP address of the DCCKI Service Interface remains constant.

2.3 The DCC shall ensure that the URL and the IP address of the DCCKI Repository Interface remains constant.

3. THE DCCKI INTERFACE CODE OF CONNECTION

Connection Mechanism

3.1 Parties that are DCCKI Eligible Subscribers in relation to Personnel Authentication Certificates may connect to the DCCKI Service Interface in accordance with the DCCKI Interface Design Specification.

3.2 Access to the DCCKI Service Interface for such Parties shall be via the Personnel Credentials Interface and shall be in accordance with the Self Service Interface Code of Connection.

3.3 The Party shall use a Supported Web Browser to access the DCCKI Service Interface.

3.4 DCC shall provide Parties' DCCKI AROs with the required URL to allow User Personnel within their organisations to access the DCCKI Service Interface via the Personnel Credentials Interface.

Management of Smart Card Tokens

3.5 Parties shall physically protect the Smart Card Token from unauthorised access and shall ensure the Smart Card Token is only used for the purpose for which it is intended.

3.6 In the event that an Administration User loses a Smart Card Token, that Administration User shall notify a DCCKI ARO for the DCCKI Subscriber. That DCCKI Subscriber shall ensure that the notified DCCKI ARO notifies the Service Desk.

3.7 DCC shall provide a replacement Smart Card Token where it receives a reasonable request for such replacement from a DCCKI ARO.

3.8 Where a Smart Card Token is no longer required, DCCKI Subscribers shall destroy that Smart Card Token beyond use and may subsequently discard it. DCCKI Subscribers shall notify the DCC of any such destruction.

3.9 Where an Administration User no longer requires access to the Self Service Interface, the DCCKI ARO shall raise an Incident in accordance with the Incident Management Policy in order to request retirement of the Self Service Interface account for that Administration User. The DCC shall ensure that this results in the revocation of the Personnel Authentication Certificate previously Issued to that Administration User.

Interface Usage

Administration Users

3.10 Administration Users shall utilise the Personnel Credentials Interface to access the DCCKI Service Interface for the purpose of obtaining a Personnel Authentication Certificate using the username and single use password provided by the DCCKI Registration Authority in accordance with the DCCKI RAPP and in accordance with the Self Service Interface Code of Connection.

User Personnel other than Administration Users

3.11 User Personnel who have accounts created for them by Administration Users shall utilise the Personnel Credentials Interface to access the DCCKI Service Interface for the purpose of obtaining a Personnel Authentication Certificate using the username and single use password provided by an Administration User in accordance with the DCCKI RAPP, and in accordance with the Self Service Interface Code of Connection.

Use of a DCCKI Infrastructure Certificate on a shared DCC Gateway Connection

3.12 DCCKI Subscribers shall notify the DCC, via the means set out on the DCC Website, of each other Party or RDP that is entitled to share (or no longer entitled to share) use of a TLS connection established using a DCCKI Infrastructure Certificate that has been Issued to that DCCKI Subscriber.

3.13 The DCC shall restrict access to the relevant DCC Interfaces, as documented in the appropriate interface specification, to DCCKI Subscribers and Parties or RDPs who have been notified to the DCC as having the entitlement to use a TLS connection established using a DCCKI Infrastructure Certificate Issued to a DCCKI Subscriber.

4. THE DCCKI REPOSITORY INTERFACE CODE OF CONNECTION

Connection Mechanism

4.1 Each Party and RDP may connect to the DCCKI Repository Interface in accordance with the DCCKI Repository Interface Design Specification.

4.2 Parties and RDPs shall use a Supported Web Browser to access the DCCKI Repository Interface.

4.3 The DCC shall provide the URL and IP address for the DCCKI Repository Interface to the DCCKI ARO of each DCCKI Authorised Subscriber.

ANNEX A

DEFINITIONS

In this document, except where the context otherwise requires:

- expressions defined in Section A of the Code (Definitions and Interpretation) have the same meaning as is set out in that section; and
- any expressions not defined here or in Section A of the Code have the meaning given to them in the DCCKI Certificate Policy, the DCCKI Registration Authority Policies and Procedures or the Self Service Access Control Interface Specification.

Smart Card Token	a physical security device used to assist authentication of User Personnel

Supported Web Browser	a web browser version that the DCC supports for use with the Self-Service Interface as listed, and as updated from time to time, in the browser policy section of the DCC Website

Version: W4.0

Appendix W

DCCKI Registration Authority Policies and Procedures (DCCKI RAPP)

Contents

1. INTRODUCTION

1.1 This DCC Key Infrastructure Registration Authority Policies and Procedures (DCCKI RAPP) sets out the activities undertaken by the DCC as the DCCKI Registration Authority in accordance with Section L of the Code, and DCCKI Certificate Policy.

1.2 This DCCKI RAPP is a SEC Subsidiary Document and is one of the DCCKI SEC Documents as set out in section L13.34 (The DCCKI SEC Documents) of the Code.

2. DCCKI ROLES

2.1 The roles of RDPs, Parties and their User Personnel in the context of access to DCCKI Services and the DCCKI Repository Service as DCCKI Authorised Subscribers, DCCKI Eligible Subscribers, and DCCKI Subscribers are set out in the Code, the DCCKI Certificate Policy (DCCKI CP), this DCCKI RAPP, and the DCCKI Code of Connection.

2.2 This DCCKI RAPP details the procedures to be followed by Parties and RDPs in respect of permitting individuals to act as DCCKI Senior Responsible Officers (DCCKI SROs) or DCCKI Authorised Responsible Officers (DCCKI AROs) on behalf of a Party or RDP.

2.3 This DCCKI RAPP also details the procedures to be followed by the DCCKI Registration Authority including in relation to the individuals acting on its behalf as DCCKI Registration Authority Managers or DCCKI Registration Authority Personnel.

2.4 Where in accordance with Section L13.22 (The DCCKI Repository Service) of the Code, the SMKI PMA makes a request for provision of a copy of any documents or information stored on the DCCKI Repository, such requests shall be made via the Service Desk. Where appropriate, the DCCKI Registration Authority shall provide the requested document(s) or information as soon as is reasonably practicable following receipt of such request.

Party and Registration Data Provider representatives

2.5 Individuals shall be permitted to act as representatives of a Party or RDP in relation to the DCCKI via the DCCKI SRO and DCCKI ARO roles as set out below.

DCCKI Senior Responsible Officer (DCCKI SRO)

2.6 In order to become and continue to be a DCCKI Authorised Subscriber each Party or RDP must have at least one individual undertaking the role of a DCCKI SRO on that organisation's behalf. A DCCKI SRO shall be an individual that:

(a) is generally authorised by the Party or RDP to fulfil the functions of a DCCKI SRO as set out in this DCCKI RAPP and elsewhere in the DCCKI SEC Documents;

(b) is specifically authorised by the Party or RDP to nominate, and de-nominate, individuals to become DCCKI AROs who may access the DCCKI Services; and

(c) has:

(i) successfully had their identity verified by the SMKI Registration Authority in accordance with the SMKI RAPP; and

(ii) successfully completed the process for becoming a DCCKI SRO on behalf of that Party or RDP in accordance with this DCCKI RAPP.

2.7 The process by which an individual is nominated, their authorisation is checked and their identity verified by the DCCKI Registration Authority, so as to be a DCCKI SRO and act on behalf of a Party or RDP, is set out in sections 3.8 to 3.11 of this DCCKI RAPP.

2.8 A DCCKI SRO may also nominate themselves to become a DCCKI ARO in accordance with section 2.9 of this DCCKI RAPP.

DCCKI Authorised Responsible Officer (DCCKI ARO)

2.9 In order to become and continue to be a DCCKI Authorised Subscriber each Party or RDP must have at least one individual undertaking the role of a DCCKI ARO on that organisation's behalf. The DCCKI SRO for a Party or RDP shall nominate at least one individual to be a DCCKI ARO in respect of that organisation, where each DCCKI ARO shall be an individual that:

(a) is generally authorised by the Party or RDP to fulfil the functions of a DCCKI ARO as set out in this DCCKI RAPP and elsewhere in the DCCKI SEC Documents;

(b) is specifically authorised to act on behalf of the Party or RDP in its capacity as a DCCKI Authorised Subscriber; and

(c) has:

(i) successfully had their identity verified by the SMKI Registration Authority in accordance with the SMKI RAPP; and

(ii) successfully completed the process for becoming a DCCKI ARO on behalf of that Party or RDP in accordance with this DCCKI RAPP.

2.10 All DCCKI AROs are also permitted to access certain DCCKI Services on behalf of the organisation that they represent.

2.11 The process by which an individual is nominated, their authorisation is checked and their identity verified by the DCCKI Registration Authority, so as to be a DCCKI ARO and act on behalf of a Party or RDP, is set out in sections 3.12 to 3.15 of this DCCKI RAPP.

The DCCKI Registration Authority

2.12 The DCC shall ensure that only individuals duly authorised to act in the role of DCCKI Registration Authority Manager or as DCCKI Registration Authority Personnel in accordance with this DCCKI RAPP shall act on behalf of the DCC in respect of matters relating to the DCCKI Registration Authority.

DCCKI Registration Authority Manager

2.13 The DCC shall nominate one or more individuals to become a DCCKI Registration Authority Manager who shall have responsibility for:

(a) management of the DCCKI Registration Authority functions, and DCCKI Registration Authority Personnel;

(b) nomination, verification, authorisation, and provision of the means for authenticating individuals to become DCCKI Registration Authority Personnel;

(c) provision of the means to authenticate access to the DCCKI Services for DCCKI Registration Authority Personnel;

(d) managing the process by which documents and information are lodged in the DCCKI Repository;

(e) approval of DCCKI Certificate Revocation Requests; and

(f) revocation of DCCKI Registration Authority Personnel credentials.

2.14 The process by which an individual is nominated, their authorisation is checked and their identity verified, so as to be a DCCKI Registration Authority Manager is set out in section 4 of this DCCKI RAPP.

DCCKI Registration Authority Personnel

2.15 A DCCKI Registration Authority Manager may nominate individuals to become DCCKI Registration Authority Personnel and to act on behalf of the DCCKI Registration Authority as set out in this DCCKI RAPP. These DCCKI Registration Authority Personnel shall, in accordance with the processes and procedures set out in this DCCKI RAPP:

(a) conduct enrolment processes in relation to Parties and RDPs, and individuals nominated to act on behalf of those Parties or RDPs, as set out in this DCCKI RAPP, incorporating assessment of whether:

(i) a nominated individual qualifies to become a DCCKI SRO or DCCKI ARO on behalf of that Party or RDP; and

(ii) a Party or RDP qualifies to become an DCCKI Authorised Subscriber.

(b) undertake the processing of:

(i) DCCKI Certificate Signing Requests;

(ii) DCCKI Certificate Revocation Requests; and

(iii) Administration User Credentials Requests; and

(c) manage the processes relating to:

(i) Parties or RDPs ceasing to be DCCKI Authorised Subscribers; and

(ii) revocation of access to the DCCKI Services by DCCKI SROs or DCCKI AROs.

2.16 The process by which an individual is nominated, their authorisation is checked and their identity verified, so as to become DCCKI Registration Authority Personnel is set out in section 4 of this DCCKI RAPP.

3. PARTY AND REGISTRATION DATA PROVIDER ENROLMENT

General enrolment obligations

Party and Registration Data Provider obligations

3.1 Each Party or RDP that wishes to use the DCCKI Services is required to become a DCCKI Authorised Subscriber.

3.2 In order to become a DCCKI Authorised Subscriber, a Party or RDP must:

(a) be an Authorised Subscriber under the Organisation Certificate Policy;

(b) submit a DCCKI Authorised Subscriber application in accordance with this DCCKI RAPP via the means set out on the DCC Website and the guidance on DCC Sharepoint;

(c) have at least one individual who is a DCCKI SRO for that Party or RDP; and

(d) have at least one individual who is a DCCKI ARO for that Party or RDP.

3.3 Each Party or RDP may:

(a) nominate multiple DCCKI SROs and multiple DCCKI AROs when requesting enrolment as a DCCKI Authorised Subscriber; and

(b) nominate additional individuals to be DCCKI SROs or DCCKI AROs at any time.

3.4 Where the information provided to the DCCKI Registration Authority in relation to:

(a) the Party or RDP being a DCCKI Authorised Subscriber;

(b) individuals who are acting in the role of DCCKI SRO for that Party or RDP; or

(c) individuals who are acting in the role of DCCKI ARO for that Party or RDP;

changes, that Party or RDP shall:

(d) advise the Service Centre, via email of such change; and

(e) ensure that the procedures as set out in section 3.27 of this DCCKI RAPP are undertaken in respect of providing revised information to the DCCKI Registration Authority, as soon as reasonably practicable thereafter.

3.5 Where a Party or RDP becomes aware that any individual ceases to be entitled to act on its behalf as either a DCCKI SRO or a DCCKI ARO in accordance with the provisions of the Code, that Party or RDP shall, as soon as reasonably practicable, follow the procedures set out in sections 3.27 to 3.30 of this DCCKI RAPP such that the DCCKI Registration Authority is able to remove the individual from its list of current DCCKI SROs and DCCKI AROs.

3.6 The DCC and any Party or RDP may agree that any action taken by either of them prior to the date of the designation of this DCCKI RAPP shall, if the equivalent action taken after that date would have satisfied a requirement of this DCCKI RAPP for the purposes of appointing a DCCKI ARO or DCCKI SRO or the Party or RDP becoming a DCCKI Authorised Subscriber, be treated as if it had taken place after that date.

DCCKI Registration Authority obligations

3.7 The DCCKI Registration Authority shall:

(a) ensure that forms that are substantively the same as those set out in Annex A to this DCCKI RAPP are made available to Parties and RDPs via the DCC Website for the purposes set out herein;

(b) provide reasonable support and advice to each Party and RDP in relation to the procedures as set out in this DCCKI RAPP, including via the DCC Website;

(c) obtain confirmation from the Registration Authority for the SMKI Services that each Party or RDP applying to be a DCCKI Authorised Subscriber is a SMKI Authorised Subscriber for Organisation Certificates;

(d) in all cases satisfy itself, via confirmation from the SMKI Registration Authority, that:

(i) any individual nominated to become a DCCKI SRO has had their identity verified in accordance with the SMKI RAPP; and

(ii) any individual nominated to become a DCCKI ARO has had their identity verified in accordance with the SMKI RAPP;

(e) where it receives a nomination for an individual to become a DCCKI SRO or a DCCKI ARO, and that individual has not had their identity verified by the SMKI Registration Authority:

(i) refer the nominated individual to the SMKI Registration Authority to allow such identity verification to be undertaken; and

(ii) provide the SMKI Registration Authority with all relevant information supplied by the nominating Party or RDP to support the identity verification;

(f) place no restriction on the number of individuals that can be nominated as DCCKI SROs or DCCKI AROs in respect of any Party or RDP;

(g) permit an individual to become a DCCKI SRO or ARO to represent multiple Parties or RDPs, by successfully completing the procedures in section 3 of this DCCKI RAPP as necessary in relation to each;

(h) not permit any individual to become a DCCKI SRO or DCCKI ARO in respect of any Party or RDP where it reasonably believes that the individual presents a material risk to DCCKICA Systems which may result in Compromise;

(i) store and maintain records relating to the nomination, verification and authorisation of individuals and organisations as set out in this DCCKI RAPP, and in accordance with the Code and the DCC's data retention policy and data protection policy;

(j) not permit any nominated individual to access the DCCKI Services on behalf of a DCCKI Authorised Subscriber until they have become a DCCKI ARO; and

(k) on successful completion of the enrolment process, provide DCCKI Authorised Subscribers and DCCKI AROs with access to the DCCKI Services in accordance with the provisions of the Code, the DCCKI CP and the DCCKI Code of Connection.

Procedure for becoming a DCCKI Senior Responsible Officer

3.8 Individuals that are an SRO in relation to SMKI Services may be nominated by the organisation that they act in that role for to become a DCCKI SRO for that same organisation.

3.9 Individuals that are not an SRO in relation to SMKI Services may be nominated to become a DCCKI SRO subject to having their identity verified by the SMKI Registration Authority in accordance with section 3.7 (e) of this DCCKI RAPP.

Submission of application

3.10 Nomination of an individual to become a DCCKI Senior Responsible Officer shall be made by a Director, Company Secretary or existing DCCKI SRO on behalf of the Party or RDP or to the level pursuant to the SMKI PMA Guidance on 'Verifying Organisation Identity'. Nomination of an individual to become a DCCKI Authorised Responsible Officer shall be made by a DCCKI Senior Responsible Officer on behalf of the Party or RDP.

(a) a DCCKI SRO Nomination Form is completed in accordance with this DCCKI RAPP and any instructions, help or advice provided by the DCCKI Registration Authority from time to time, including via the DCC Website;

(b) the information provided is complete and accurate;

(c) the DCCKI SRO Nomination Form is authorised by a Director, or Company Secretary of that Party or RDP; and

(d) the completed DCCKI SRO Nomination Form is submitted to the DCCKI Registration Authority via the means set out on the DCC Website.

DCCKI Registration Authority processing of DCCKI SRO nominations

3.11 On receipt of a duly completed DCCKI SRO Nomination Form, the DCCKI Registration Authority shall, as soon as is reasonably practicable:

(a) acknowledge receipt via the Service Desk to the individual who submitted the DCCKI SRO Nomination Form via telephone or in writing, using the contact details provided on that form;

(b) satisfy itself that:

(i) the Party or RDP has provided all required information to allow the application to be progressed; and

(ii) the individual nominated to become a DCCKI SRO is an SRO in relation to SMKI Services in respect of the nominating Party or RDP or has had their identity verified by the SMKI Registration Authority, as evidenced by confirmation of this fact by the SMKI Registration Authority;

(c) contact the individual via the Service Desk who submitted the DCCKI SRO Nomination Form, via telephone or in writing, using contact details as provided, to confirm whether the application has been successful or unsuccessful;

(d) either:

(i) notify the Director or Company Secretary via the Service Desk that authorised the DCCKI SRO Nomination Form that the application has been unsuccessful, in writing; or

(ii) notify the Director or Company Secretary via the Service Desk that authorised the DCCKI SRO Nomination Form that the application has been successful, in writing; and

(e) where the application has been successful, add the relevant individual to the DCCKI Registration Authority list of DCCKI SROs maintained in accordance with the DCCKI CPS.

Procedure for becoming a DCCKI Authorised Responsible Officer

3.12 Individuals that are AROs in relation to SMKI Services may be nominated by the organisation that they act in that role for to become a DCCKI ARO for that same organisation.

3.13 Individuals that are not an ARO in relation to SMKI Services may be nominated to become a DCCKI ARO subject to having their identity verified by the SMKI Registration Authority in accordance with section 3.7 (e) of this DCCKI RAPP.

Submission of DCCKI ARO nomination

3.14 Where a Party or RDP wishes to nominate an individual to become a DCCKI ARO, a DCCKI SRO, Director or Company Secretary of that Party or RDP shall ensure that:

(a) a DCCKI ARO Nomination Form is completed in accordance with this DCCKI RAPP and any instructions, help or advice provided by the DCCKI Registration Authority from time to time, including via the DCC Website;

(b) the information provided is complete and accurate;

(c) the DCCKI ARO Nomination Form is authorised by a DCCKI SRO, Director or Company Secretary; and

(d) the completed DCCKI ARO Nomination Form in submitted to the DCCKI Registration Authority via the means set out on the DCC Website.

DCCKI Registration Authority processing of DCCKI ARO nominations

3.15 On receipt of a duly completed DCCKI ARO Nomination Form, the DCCKI Registration Authority shall, as soon as is reasonably practicable:

(a) acknowledge receipt via the Service Desk to the DCCKI SRO, Director or Company Secretary who submitted the DCCKI ARO Nomination Form via telephone or in writing, using the contact details provided on that form;

(b) satisfy itself that:

(i) the Party or RDP has provided all required information to allow the application to be progressed; and

(ii) the individual nominated to become an DCCKI ARO is an ARO in relation to SMKI Services in respect of the nominating Party or RDP or has had their identity verified by the SMKI Registration Authority, as evidenced by confirmation of this fact by the SMKI Registration Authority;

(c) contact the DCCKI SRO, Director or Company Secretary via the Service Desk who submitted the DCCKI ARO Nomination Form, via telephone or in writing, using contact details as provided, to confirm whether the application has been successful;

(d) either:

(i) notify the DCCKI SRO, Director or Company Secretary via the Service Desk that authorised the DCCKI ARO Nomination Form that the application has been unsuccessful, in writing; or

(ii) notify the DCCKI SRO, Director or Company Secretary via the Service Desk that authorised the DCCKI ARO Nomination Form that the application has been successful, in writing; and

(e) where the application has been successful, add the relevant individual to the DCCKI Registration Authority list of DCCKI AROs maintained in accordance with the DCCKI CPS.

Procedure for becoming a DCCKI Authorised Subscriber

Submission of request

3.16 Where a Party or RDP wishes to become a DCCKI Authorised Subscriber, a Director, Company Secretary or DCCKI SRO of that Party or RDP shall ensure that:

(a) a DCCKI Authorised Subscriber Application is submitted in accordance with this DCCKI RAPP and any instructions, help or advice provided by the DCCKI Registration Authority from time to time, including via the DCC Website, and including the provision of such information as is set out in the form contained in Annex A (A3) to this DCCKI RAPP;

(b) the information provided is complete and accurate;

(c) the DCCKI Authorised Subscriber Application is authorised by a Director or Company Secretary of that Party or RDP, or DCCKI SRO; and

(d) the DCCKI Authorised Subscriber Application is submitted to the DCCKI Registration Authority via the means set out on the DCC Website.

DCCKI Registration Authority processing of DCCKI Authorised Subscriber Applications

3.17 On receipt of a DCCKI Authorised Subscriber Application, the DCCKI Registration Authority shall, as soon as is reasonably practicable thereafter:

(a) acknowledge receipt via the Service Desk to the individual who submitted that DCCKI Authorised Subscriber Application via telephone or in writing, using the contact details provided as part of the submission;

(b) satisfy itself that the Party or RDP:

(i) has provided all required information to allow the DCCKI Authorised Subscriber Application to be progressed; and

(ii) is an Authorised Subscriber in relation to Organisation Certificates, as evidenced by confirmation of this fact by the SMKI Registration Authority;

(c) satisfy itself that no material risk of Compromise to any part of the DCC Systems would result from permitting the Party or RDP to become a DCCKI Authorised Subscriber;

(d) contact the individual who submitted the DCCKI Authorised Subscriber Application, via telephone or in writing, using contact details as provided, to confirm whether the application has been successful;

(e) either:

(i) notify the Director, Company Secretary or DCCKI SRO via the Service Desk that authorised the DCCKI Authorised Subscriber Application that the application has been unsuccessful, in writing; or

(ii) notify the Director, Company Secretary or DCCKI SRO via the Service Desk that authorised the DCCKI Authorised Subscriber Application that the application has been successful, in writing;

(f) where the application has been successful, enable access to the DCCKI Services for the relevant Party or RDP in accordance the provisions of the Code, the DCCKI CP and the DCCKI Code of Connection; and

(g) add the relevant Party or RDP to the DCCKI Registration Authority list of DCCKI Authorised Subscribers maintained in accordance with the DCCKI CPS.

Procedure for providing credentials to DCCKI AROs in order to allow Administration Users to use the Self Service Interface

3.18 In order to obtain access to the Self Service Interface (SSI) in accordance with the Self Service Interface Access Control Specification, each DCCKI Authorised Subscriber that is a DCCKI Eligible Subscriber in relation to Personnel Authentication Certificates may submit an Administration User Credentials Request in order to obtain credentials for a member of the User Personnel of that organisation nominated to become an Administration User via the procedures set out immediately below.

Submission of Administration User Credentials Requests

3.19 A DCCKI ARO of a DCCKI Authorised Subscriber that meets the conditions set out in section 3.18 of this DCCKI RAPP may submit an Administration User Credentials Request to the DCCKI Registration Authority using the form provided for the purpose on the DCC Website, which shall be substantively in the form set out in Annex A (A5) to this DCCKI RAPP.

3.20 In submitting an Administration User Credentials Request, a DCCKI ARO of a DCCKI Subscriber shall provide the required details of the User Personnel who are to be provided with Smart Card Tokens, single use passwords and usernames for the purposes of establishing access to the Personnel Credentials Interface, and submitting a Personnel Authentication Certificate Application as Administration Users.

DCCKI Registration Authority processing of Administration User Credentials Requests

3.21 On receipt of an Administration User Credentials Request, DCCKI Registration Authority Personnel shall;

(a) confirm via the Service Desk to the DCCKI ARO that submitted the request that such request has been received, where this notification may be made via telephone or in writing using the contact details established as part of enrolment to the DCCKI Services;

(b) ensure that the submitting organisation meets the conditions set out in section 3.18 of this DCCKI RAPP; and

(c) ensure that all required information has been provided.

3.22 Where the Administration User Credentials Request is valid, the DCCKI Registration Authority shall in relation to that request:

(a) ensure that single use passwords and usernames are generated for each member of User Personnel whose details are provided;

(b) provide, via a secured electronic means as set out on the DCC Website, the usernames to be associated with those User Personnel for the purpose of accessing the Personnel Credentials Interface;

(c) provide, via secure post, the single use passwords to be associated with those User Personnel for the purpose of accessing the Personnel Credentials Interface; and

(d) provide one Smart Card Token for each member of User Personnel identified:

(i) to the DCCKI ARO that submitted the request or their named alternative, whose details have been provided by that DCCKI ARO at the time the request was made. This delivery may be in person, via a nominated employee, or via a commercial courier service. (Any person delivering the materials shall have information that enables verification of the materials and the sending organisation, and allows authentication of that person's identity); and

(ii) ensure that the DCCKI ARO that submitted the request (or their named alternative) is advised in advance of any such delivery, including the means of delivery, and the name of the person that shall be making that delivery. This notification may be made via telephone or in writing using the contact details established as part of enrolment to the DCCKI Services.

3.23 If the Administration User Credentials Request is not valid, the DCCKI Registration Authority Manager shall ensure that a DCCKI SRO of the submitting organisation and the DCCKI ARO who submitted that request is notified of the reasons for its rejection.

Establishment of Administration User credentials

3.24 On receipt of the Smart Card Tokens, usernames and single use passwords from the DCCKI Registration Authority, the DCCKI ARO shall ensure the distribution of the required materials to the relevant User Personnel within their organisation. Those User Personnel may then use the materials to access the Personnel Credentials Interface for the purposes of submitting a Personnel Authentication Certificate Application and obtaining a Personnel Authentication Certificate in accordance with the procedures set out in the DCCKI Interface Design Specification.

3.25 Following successfully obtaining a Personnel Authentication Certificate, the User Personnel nominated by that DCCKI ARO shall be an enabled Administration User who may then create usernames and single use passwords for other User Personnel within their organisation in accordance with the DCCKI Interface Design Specification.

3.26 In the event that, following provision of Smart Card Tokens, usernames and single use passwords by a DCCKI ARO, relevant User Personnel are unable to successfully obtain a Personnel Authentication Certificate, that DCCKI ARO shall raise an Incident in accordance with the Incident Management Policy, in order to resolve the matter.

Maintenance of information relating to DCCKI SROs and DCCKI AROs

Procedures for providing changes in information relating to DCCKI SROs and DCCKI AROs

3.27 Where either:

(a) the contact details provided to the DCCKI Registration Authority for a DCCKI SRO or DCCKI ARO change; or

(b) a Party or RDP determines that a DCCKI SRO or DCCKI ARO is no longer entitled to act as such in relation to that organisation;

a DCCKI SRO, a Director or Company Secretary of that Party or RDP shall notify the DCCKI Registration Authority in accordance with section 3.28 below.

3.28 The Party or RDP making the notification shall contact the DCCKI Registration Authority via the means set out on the Website, and provide the following information:

(a) the name of the person making the notification, their contact details and the name of the organisation that they represent;

(b) the name of the DCCKI SRO or DCCKI ARO whose details require amendment; and

(c) whether that DCCKI SRO or DCCKI ARO is still entitled to act as such on behalf of the notifying Party or RDP.

3.29 On receipt of updated information from a Party or RDP, the DCCKI Registration Authority shall, as soon as is reasonably practicable:

(a) acknowledge receipt in writing via the Service Desk to the person making the notification;

(b) verify the completeness of the information contained in the notification;

(c) contact the DCCKI SRO, a Director or Company Secretary via the Service Desk of that Party making the notification by telephone or in writing using the registered contact details for the DCCKI SRO, a Director or Company Secretary of that Party as held by the DCCKI Registration Authority to confirm the notification is authorised;

(d) amend its records in accordance with the information received; and

(e) provide confirmation in writing via the Service Desk to both the individual who made the notification, and the relevant DCCKI SRO or DCCKI ARO that the DCCKI Registration Authority has made the requested updates, and what those updates are.

DCCKI Registration Authority Amendments to DCCKI SRO or DCCKI ARO Information

3.30 In circumstances where:

(a) the DCCKI Registration Authority reasonably believes that a DCCKI SRO or DCCKI ARO has materially failed to comply with the DCCKI policies as set out in the DCCKI Certificate Policy, this DCCKI RAPP, or the Code; and

(b) that individual has been notified of the fact by the DCCKI Registration Authority including the nature of the non-compliance;

the DCCKI Registration Authority may amend its records such that the individual is no longer authorised to act in the role of a DCCKI SRO or DCCKI ARO for a Party or RDP as the case may apply.

3.31 Where the DCCKI Registration Authority has amended its records in accordance with section 3.30 of this DCCKI RAPP, it shall inform the relevant individual of the fact, and:

(a) in the case of a DCCKI SRO, inform a Director or Company Secretary of the relevant DCCKI Authorised Subscriber using the registered contact details of the Director or Company Secretary of that Party as held by the DCCKI Registration Authority; or

(b) in the case of a DCCKI ARO, inform a DCCKI SRO of the relevant DCCKI Authorised Subscriber.

Reapplying to be a DCCKI SRO or DCCKI ARO

3.32 In circumstances where an individual has ceased to be a DCCKI SRO or a DCCKI ARO for a Party or RDP, nothing shall preclude them from re-applying to become a DCCKI SRO or DCCKI ARO on behalf of that or another Party or RDP by following the procedures set out in this DCCKI RAPP.

4. DCCKI REGISTRATION AUTHORITY ENROLMENT PROCEDURES

4.1 The procedures set out in this section 4 shall be undertaken in order for nominated individuals to act on behalf of the DCCKI Registration Authority as either a DCCKI Registration Authority Manager or a member of DCCKI Registration Authority Personnel.

General registration obligations

4.2 The DCC shall be responsible for ensuring that only those individuals authorised in accordance with the DCCKI CP, the DCCKI CPS, and this DCCKI RAPP are appointed to the roles of DCCKI Registration Authority Manager and DCCKI Registration Authority Personnel. The DCC shall ensure that its CISO ensures that such authorisations are made in accordance with the procedures set out in this DCCKI RAPP.

4.3 In respect of DCCKI Registration Authority Managers and DCCKI Registration Authority Personnel, the DCCKI Registration Authority shall:

(a) not permit any individual to access DCCKICA Systems used to provide DCCKI Services or DCCKI Repository Services as a DCCKI Registration Authority Manager or member of DCCKI Registration Authority Personnel until the procedures in this section 4 of this DCCKI RAPP are successfully completed;

(b) store and maintain records relating to individuals becoming DCCKI Registration Authority Managers and DCCKI Registration Authority Personnel, in accordance with the Code and DCC data retention policy;

(c) ensure that there is at least one DCCKI Registration Authority Manager at all times;

(d) if there is a change to any of the information used to verify the identity of any DCCKI Registration Authority Manager or member of DCCKI Registration Authority Personnel, ensure that the relevant DCCKI Registration Authority Manager or member of DCCKI Registration Authority Personnel undertakes the procedures as set out in this DCCKI RAPP in respect of the revised evidence of identity; and

(e) ensure that authentication credentials provided to DCCKI Registration Authority Managers and DCCKI Registration Authority Personnel in accordance with section 4.12 of this DCCKI RAPP shall expire three years following issuance of such authentication credentials.

Procedure for becoming a Registration Authority Manager

4.4 The DCC CISO, or an individual they have authorised on their behalf to act in this capacity, shall be responsible for:

(a) nomination of individuals to fulfil the role of DCCKI Registration Authority Manager;

(b) confirmation to each nominated individual of a location, date and time for a verification meeting, to be held at DCC premises; and

(c) advising each nominated individual of the evidence to be provided in order to verify their identity.

4.5 At the verification meeting, DCC shall:

(a) check proof of identity provided against the information provided by the nominated individual; and

(b) verify the identity of the nominated individual in accordance with the provisions of Section G4.6 (Obligations on the DCC) of the Code.

4.6 Where the identity of the nominated individual is not successfully verified, DCC shall:

(a) provide reasons for the failure to the individual and the DCC CISO; and

(b) notify the individual that a further verification meeting is required to remedy the unsuccessful elements of the verification.

4.7 Where the identity of the nominated individual is successfully verified, DCC shall:

(a) notify the individual verbally and subsequently make notification in writing to both the individual and the DCC CISO that the individual has become a DCCKI Registration Authority Manager;

(b) record the details of the individual that has become a DCCKI Registration Authority Manager; and

(c) provide the DCCKI Registration Authority Manager with credentials as defined in the DCCKI CPS to be used to perform activities on behalf of the DCCKI Registration Authority.

Procedure for becoming a member of Registration Authority Personnel

4.8 The DCCKI Registration Authority Manager, acting on behalf of the DCCKI Registration Authority, shall:

(a) nominate individuals to become members of DCCKI Registration Authority Personnel;

(b) confirm a location date and time for a verification meeting, to be held at DCC premises to each nominated individual; and

(c) advise each nominated individual of the evidence to be provided in order to verify their identity.

4.9 At the agreed verification meeting, the DCCKI Registration Authority Manager shall:

(a) check proof of identity provided against the information provided by the nominated individual; and

(b) verify the identity of the nominated individual in accordance with the provisions of Section G4.6 (Obligations on the DCC) of the Code.

4.10 Where the identity of the nominated individual is not successfully verified, the DCCKI Registration Authority Manager shall:

(a) provide reasons for the failure to the individual; and

(b) notify the individual that a further verification meeting is required to remedy the unsuccessful elements of the verification.

4.11 Where the identity of the nominated individual is successfully verified, the DCCKI Registration Authority Manager shall:

(a) notify the individual verbally and subsequently in writing that they have become a member of DCCKI Registration Authority Personnel;

(b) record the details of the individual that has become a member of DCCKI Registration Authority Personnel; and

(c) provide the member of DCCKI Registration Authority Personnel with credentials as defined in the DCCKI CPS to be used to perform activities on behalf of the DCCKI Registration Authority.

Procedure for provision of credentials to a Registration Authority Manager or a Registration Authority Personnel

4.12 The DCC shall ensure that the DCCKI CPS details the procedure for provision of credentials to a DCCKI Registration Authority Manager or DCCKI Registration Authority Personnel.

5. SUBMISSION OF REQUESTS FOR AND ISSUANCE OF DCCKI CERTIFICATES

General DCCKI Registration Authority Obligations

5.1 The DCCKI Registration Authority shall ensure that:

(a) no DCCKICA Certificates are signed using a Root DCCKICA Private Key after the expiry of the Validity Period of the corresponding Root DCCKICA Certificate;

(b) no DCCKI Infrastructure Certificates are Issued using a EII DCCKICA Private Key after the expiry of the Validity Period of the corresponding EII DCCKICA Certificate;

(c) no Personnel Authentication Certificates are Issued using a UI DCCKICA Private Key after the expiry of the Validity Period of the corresponding UI DCCKICA Certificate;

(d) DCCKI Certificates are Issued only in accordance with the provisions set out in this DCCKI RAPP, the DCCKI Certificate Policy, and the DCCKI Interface Design Specification;

(e) each EII DCCKICA Certificate and UI DCCKICA Certificate that is Issued by the Root DCCKI CA has been verified to be correct and complete;

(f) each DCCKI Infrastructure Certificate that is Issued by the EII DCCKICA has been verified to be correct and complete and complies with the DCCKI Certificate Signing Request received;

(g) each Personnel Authentication Certificate that is Issued by the UI DCCKICA has been verified to be correct and complies with the Personnel Certificate Application received via the Personnel Credentials Interface;

(h) all DCCKI Infrastructure Certificates shall be Issued within one (1) Working Day of receipt of a valid DCCKI Certificate Signing Request from a DCCKI Eligible Subscriber;

(i) all Personnel Authentication Certificates shall be Issued as soon as is reasonably possible following the receipt of a valid Personnel Authentication Certificate Application;

(j) a record of all DCCKI Certificates which have been Issued by the DCCKICA and accepted by a DCCKI Eligible Subscriber is maintained;

(k) the Root DCCKICA Certificate and EII DCCKICA Certificate are made available to DCCKI Relying Parties via the DCCKI Repository; and

(l) the name of the subject of each DCCKI Certificate that is Issued is consistent with the information provided via the DCCKI Certificate Signing Request or Personnel Authentication Application received via the Personnel Credentials Interface as the case may be.

General DCCKI Eligible Subscriber Obligations

5.2 DCCKI Authorised Subscribers that are DCCKI Eligible Subscribers in respect of DCCKI Infrastructure Certificates as set out in the DCCKI CP may submit DCCKI Certificate Signing Requests in accordance with the procedures set out in this DCCKI RAPP, the DCCKI Interface Design Specification and the DCCKI Code of Connection.

5.3 In the case of DCCKI Infrastructure Certificates, a DCCKI Eligible Subscriber may only request Issuance via submission of a DCCKI Certificate Signing Request and where that DCCKI Eligible Subscriber is a SMKI Subscriber in relation to an Organisation Certificate in accordance with section 5.6 of this DCCKI RAPP.

5.4 In the case of Personnel Authentication Certificates, a DCCKI Eligible Subscriber may only submit a Personnel Authentication Certificate Application via the Personnel Credentials Interface in accordance with the provisions of the DCCKI Interface Design Specification.

DCCKI Certificate Signing Requests

5.5 DCCKI Certificate Signing Requests may only be submitted by a DCCKI ARO of the DCCKI Eligible Subscriber, and in relation to DCCKI Infrastructure Certificates.

5.6 In submitting a DCCKI Certificate Signing Request, a DCCKI ARO of a DCCKI Eligible Subscriber shall:

(a) generate a Key Pair within a Cryptographic Module;

(b) generate a DCCKI Certificate Signing Request, containing the attributes and format defined within the DCCKI Interface Design Specification, and in accordance with the DCCKI CP;

(c) ensure that the DCCKI Certificate Signing Request is Digitally Signed using the Private Key associated with the Public Key contained in the DCCKI Certificate Signing Request in accordance with PKCS#10;

(d) verify the accuracy of details contained within the DCCKI Certificate Signing Request and on success, shall use the Private Key associated with the corresponding Public Key in an Organisation Certificate for which it is a Subscriber to Digitally Sign the DCCKI Certificate Signing Request as set out in the DCCKI Interface Design Specification; and

(e) send the DCCKI Certificate Signing Request to the DCCKI Registration Authority via secured electronic means as set out on the DCC Website.

5.7 As soon as reasonably practicable following receipt of the DCCKI Certificate Signing Request, the DCCKI Registration Authority Personnel shall acknowledge receipt in writing via the Service Desk to the DCCKI ARO who submitted the DCCKI Certificate Signing Request, using the contact details established as part of enrolment to the DCCKI Services.

Authentication of DCCKI Certificate Signing Requests

5.8 DCCKI Registration Authority Personnel shall validate that for each DCCKI Certificate Signing Request submitted:

(a) the organisation submitting the DCCKI Certificate Signing Request is a DCCKI Eligible Subscriber in relation to DCCKI Infrastructure Certificates in accordance with the DCCKI CP;

(b) the format of the DCCKI Certificate Signing Request is valid in relation to requests for DCCKI Certificates as specified in the DCCKI Interface Design Specification; and

(c) the DCCKI Certificate Signing Request is correctly signed in accordance with section 5.6 of this DCCKI RAPP.

5.9 If a DCCKI Certificate Signing Request so submitted is not valid, the DCCKI Registration Authority shall reject the DCCKI Certificate Signing Request, and shall follow the process for the rejection of DCCKI Certificate Signing Request set out in this DCCKI RAPP.

5.10 Where the DCCKI Certificate Signing Request is valid, the DCCKI Registration Authority shall submit it to the EII DCCKICA.

Rejection of DCCKI Certificate Signing Requests

5.11 Rejection of a DCCKI Certificate Signing Request may occur where:

(a) the DCCKI Certificate Signing Request cannot be validated in accordance with section 5.8 of this DCCKI RAPP; or

(b) the DCCKI Certificate Signing Request is not compliant with the DCCKI CP, the DCCKI Interface Design Specification or other provisions of the Code.

5.12 In the event of a DCCKI Certificate Signing Request being rejected, the DCCKI Registration Authority shall:

(a) create a record of the rejection on the DCCKI Certificate Signing Request Rejection Form, which shall contain the information and be substantively as set out in Annex A (A4) to this DCCKI RAPP;

(b) notify a DCCKI ARO of the organisation via the Service Desk that submitted the DCCKI Certificate Signing Request of its rejection, this may be via telephone or in writing, using the contact details established as part of enrolment for the DCCKI Services; and

(c) provide a copy of the DCCKI Certificate Signing Request Rejection Form via secured electronic means as set out on the DCC Website.

Certificate Issuance in response to a DCCKI Certificate Signing Request

5.13 Upon successful validation of the information provided in the DCCKI Certificate Signing Request by the DCCKI Registration Authority, the EII DCCKICA, shall generate the DCCKI Infrastructure Certificate based on the information contained within the DCCKI Certificate Signing Request.

5.14 Following Issuance of the DCCKI Infrastructure Certificate, the DCCKI Registration Authority shall:

(a) publish the DCCKI Infrastructure Certificate to the DCCKI Repository in accordance with the DCCKI CP; and

(b) notify the DCCKI ARO via the Service Desk that submitted the DCCKI Certificate Signing Request of its Issuance, in writing, using the contact details established as part of enrolment for the DCCKI Services.

Acceptance or Rejection of DCCKI Certificates Issued following a DCCKI Certificate Signing Request submission

5.15 As soon as is reasonably practicable following notification of Issuance of a DCCKI Infrastructure Certificate as set out in section 5.14 above, the DCCKI Eligible Subscriber that submitted the DCCKI Certificate Signing Request shall:

(a) validate the DCCKI Infrastructure Certificate published on the DCCKI Repository; and

(b) notify the DCCKI Registration Authority if the DCCKI Infrastructure Certificate is rejected, in writing, using the contact details established as part of the enrolment of the DCCKI Services.

5.16 Where the DCCKI Registration Authority receives a valid notification of the rejection of a DCCKI Infrastructure Certificate, it shall revoke that DCCKI Infrastructure Certificate in accordance with the procedures set out in section 6 of this DCCKI RAPP.

5.17 Not In Use.

Personnel Authentication Certificate Application

5.18 Provision is made in the DCCKI Interface Design Specification in relation to the mechanism by which a DCCKI Eligible Subscriber may request a Personnel Authentication Certificate Application. Prior to requesting a Personnel Authentication Certificate Application, DCCKI Eligible Subscribers shall follow the procedures set out in sections 3.18 to 3.26 of this DCCKI RAPP.

Issuance of User Personnel Authentication Certificates

5.19 Personnel Authentication Certificates shall be Issued to User Personnel following a Personnel Authentication Certificate Application via the Personnel Credentials Interface.

5.20 User Personnel of DCCKI Eligible Subscribers who are not Administration Users shall have the Private Key associated with the Personnel Authentication Certificate delivered to them along with the Personnel Authentication Certificate in accordance with the DCCKI Interface Design Specification.

5.21 The DCCKI Interface Design Specification sets out further provisions in respect of the circumstances in which the UI DCCKICA shall Issue Personnel Authentication Certificates.

Rejection and Acceptance of a Personnel Authentication Certificate

5.22 Use of the Private Key associated with a Personnel Authentication Certificate to Authenticate to the SSI shall be deemed to constitute acceptance of the Personnel Authentication Certificate by the DCCKI Eligible Subscriber.

5.23 To reject a Personnel Authentication Certificate, a DCCKI Eligible Subscriber shall raise an Incident in accordance with the Incident Management Process.

5.24 Where the DCCKI Registration Authority receives a valid notification of the rejection of a Personnel Authentication Certificate, it shall revoke that Personnel Authentication Certificate in accordance with the procedures set out in section 6 of this DCCKI RAPP.

6. REVOCATION

DCCKI Certificate Revocation

6.1 The circumstances under which DCCKI Subscribers and the DCC may request revocation of a DCCKI Certificate are set out in the DCCKI CP. In all cases, the procedures set out in this DCCKI RAPP shall be followed in respect of DCCKI Certificate revocation.

6.2 Where DCC reasonably believes that there has been a material breach of obligations under the Code that could lead to a material Compromise of DCC Systems, it may request revocation of the DCCKI Certificates issued to the relevant Party or RDP. This revocation shall not preclude the affected Party or RDP from applying for further DCCKI Certificates once any material breach has been remedied, or following any determination to the contrary by the Panel.

Revocation of DCCKI Infrastructure Certificate

6.3 Each DCCKI Relying Party shall raise an Incident as soon as possible following awareness of Compromise or suspected Compromise of any DCCKI Infrastructure Certificate.

6.4 On notification of an Incident, the DCC may raise a DCCKI Certificate Revocation Request via the procedure set out in section 6.8 and 6.9 below in response to the Incident. Any grace period during which the relevant DCCKI Infrastructure Certificates are not revoked shall be agreed at the time that the DCCKI Certificate Revocation Request is made.

6.5 Where a DCCKI Subscriber is aware of Compromise or suspected Compromise of a DCCKI Infrastructure Certificate Issued to it, the DCCKI Subscriber shall request revocation of that DCCKI Infrastructure Certificate in accordance with sections 8 and 9 of this DCCKI RAPP, and raise an Incident as soon as reasonably practicable.

6.6 Where the DCCKI Registration Authority Personnel has issued a DCCKI Infrastructure Certificate incorrectly the DCCKI Infrastructure Certificate may be revoked provided;

(a) the certificate has not been issued to an DCCKI ARO; and

(b) the revocation request is approved by a the DCCKI Registration Authority Manager.

6.7 Where the DCCKI Registration Authority Personnel has issued a DCCKI Infrastructure Certificate incorrectly and it has been issued to the DCCKI ARO the DCCKI Infrastructure Certificate may be revoked provided:

(a) an incident is raised; and

(b) the requesting DCCKI ARO is notified and a new Certificate Signing Request is submitted;

Procedure for DCCKI Certificate Revocation Requests

6.8 DCCKI Certificate Revocation Requests shall be made in writing, via the means set out on the DCC Website, to the DCCKI Registration Authority.

6.9 A DCCKI Certificate Revocation Request shall:

(a) identify the DCCKI Subscriber;

(b) identify the individual making the request, and their role, which shall be:

(i) in the case of a DCCKI Subscriber, a DCCKI SRO of that organisation; or

(ii) in the case of the DCC, the DCC CISO, or an individual that they have authorised to act on their behalf in this capacity;

(c) identify the DCCKI Certificate to be revoked; and

(d) state the criteria for the revocation.

6.10 On receipt of a valid DCCKI Certificate Revocation Request, the DCCKI Registration Authority shall:

(a) validate the revocation request by contacting:

(i) in the case of a DCCKI Subscriber, the DCCKI SRO, using the contact details of the DCCKI SRO as provided in the original application to become a DCCKI SRO; or

(ii) in the case of the DCC, the DCC CISO, using the registered contact details for the DCC CISO as held by the DCCKI Registration Authority

to confirm that the DCCKI Certificate Revocation Request is authentic;

(b) where the validation is unsuccessful, reject the DCCKI Certificate Revocation Request and notify the DCCKI SRO or the DCC CISO via the Service Desk of the rejection;

(c) where the validation is successful, notify the DCCKI SRO or the DCC CISO via the Service Desk of the acceptance of the DCCKI Certificate Revocation Request, and then:

(i) revoke the DCCKI Infrastructure Certificate;

(ii) update the EII DCCKICA CRL and lodge the updated EII DCCKICA CRL in the DCCKI Repository; and

notify the DCCKI SRO or the DCC CISO of the revocation via the Service Desk.

Revocation of Personnel Authentication Certificates

6.11 If a Personnel Authentication Certificate is suspected of Compromise, the DCCKI Subscriber shall request a new Personnel Authentication Certificate in accordance with this DCCKI RAPP and the DCCKI Interface Design Specification.

6.12 On receipt of a new Personnel Authentication Certificate Application for a User Personnel already Issued with a Personnel Authentication Certificate, the UI DCCKICA shall revoke the existing Personnel Authentication Certificate.

6.13 Retirement of an SSI account for a member of a Party's User Personnel shall result in the revocation of the Personnel Authentication Certificate associated with that SSI account.

Ceasing to be a DCCKI Authorised Subscriber

6.14 A Party or RDP shall cease to be a DCCKI Authorised Subscriber where:

(a) that Party or RDP makes a request to the DCCKI Registration Authority to cease to be a DCCKI Authorised Subscriber;

(b) the DCC reasonably believes that Party or RDP, or any of its DCCKI SROs or DCCKI AROs as individuals, have failed or are failing materially to comply with the DCCKI policies as set out in the DCCKI Certificate Policy, this DCCKI RAPP, or any other provision of the Code such that there is a material risk of Compromise to the DCC Systems; or

(c) they fail to have in place at any time at least one DCCKI SRO and at least one DCCKI ARO.

6.15 Where a Party or RDP ceases to be a DCCKI Authorised Subscriber, the DCCKI Registration Authority shall:

(a) notify the Party or RDP via the Service Desk, giving reasons for why it has ceased to be a DCCKI Authorised Subscriber;

(b) update its list of DCCKI Authorised Subscribers; and

(c) revoke all DCCKI Certificates that have been Issued to that Party or RDP, in accordance with this DCCKI RAPP.

ANNEX A – FORM TEMPLATES

The Form Templates listed in Appendix A are available from the DCC Website or via SharePoint as provided by the DCC.

The DCC may, subject to the approval of the SMKI PMA, modify the form templates from time to time.

A1. DCCKI SRO NOMINATION FORM

A2. DCCKI ARO NOMINATION FORM

A3. DCCKI AUTHORISED SUBSCRIBER APPLICATION FORM

A4. DCCKI CERTIFICATE SIGNING REQUEST REJECTION FORM

A5. ADMINISTRATION USER CREDENTIALS REQUEST FORM

A6. DCCKI CERTIFICATE REVOCATION REQUEST FORM

ANNEX B DEFINED TERMS

In this DCCKI RAPP, except where the context otherwise requires:

- expressions defined in Section A of the Code (Definitions and Interpretation) have the same meaning as is set out in that Section;
- the expressions in the left hand column below shall have the meanings given to them in the right hand column below; and
- where any expression is defined in Section A of the Code (Definitions and Interpretation) and in this Annex, the definition in this Annex shall take precedence for the purposes of this document.

Definitions for this DCCKI RAPP

Administration User Credentials Request	means a request submitted by a DCCKI ARO for the provision of Smart Card Tokens, usernames and single use passwords to be utilised by User Personnel nominated to be an Administration User.
Authorised Responsible Officer	has the meaning given to that expression in the SMKI RAPP.
Authenticate	has the meaning given to that term in the DCCKI Certificate Policy.
CISO	means chief information security officer
DCCKI Authorised Responsible Officer (DCCKI ARO)	means an individual that has successfully completed the process for becoming a DCCKI ARO on behalf of a party or RDP in accordance with this DCCKI RAPP.
DCCKI ARO Nomination Form	means the form of that name as provided via the DCC Website which shall be used by Parties and RDPs wishing to nominate individuals to act as a DCCKI ARO on their behalf.
DCCKI Authorised Subscriber Application	means a request to become a DCCKI Authorised Subscriber submitted by a Party or RDP in accordance with the procedures set out in the DCCKI RAPP.

DCCKICA Systems	has the meaning given to that expression in the DCCKI Certificate Policy.
DCCKI Certificate Revocation Request	has the meaning given to that expression in the DCCKI Certificate Policy.
DCCKI Certificate Signing Request Rejection Form	means the form of that name as set out in Annex A (A6) to the DCCKI RAPP and used by the DCCKI Registration Authority to inform a DCCKI Authorised Subscriber for the reasons for rejection of a DCCKI Certificate Signing Request or DCCKI Certificate Application.
DCCKI Registration Authority Manager	means an individual who acts on behalf of the DCCKI Registration Authority to perform tasks relating to the management of the DCCKI Registration Authority, as set out in the DCCKI RAPP.
DCCKI Registration Authority Personnel	means those persons who are engaged by DCC, in so far as such persons carry out functions of the DCCKI Registration Authority as set out in the DCCKI RAPP.
DCCKI Senior Responsible Officer (DCCKI SRO)	means an individual that has successfully completed the process for becoming a DCCKI SRO on behalf of a Party or RDP in accordance with this DCCKI RAPP.
DCCKI SRO Nomination Form	means the form of that name as provided via the DCC Website which shall be used by Parties and RDPs wishing to nominate individuals to act as a DCCKI SRO on their behalf.
EII DCCKICA	has the meaning given to that expression in the DCCKI Certificate Policy.
EII DCCKICA Private Key	has the meaning given to that expression in the DCCKI Certificate Policy.
Personnel Credentials Interface	means the interface that allows for the activation of user accounts, the submission of Personnel Authentication Certificate Applications, and the provision of Personnel Authentication Certificates to persons.
Root DCCKICA	has the meaning given to that expression in the DCCKI Certificate Policy.
Root DCCKICA Private Key	has the meaning given to that expression in the DCCKI Certificate Policy.
Smart Card Token	a physical security device used to assist authentication of User Personnel
Senior Responsible Officer (SRO)	has the meaning given to that expression in the SMKI RAPP.
SMKI Registration Authority	has the meaning given to that expression in the SMKI RAPP.

UI DCCKICA	has the meaning given to that expression in the DCCKI Certificate Policy.

UI DCCKICA Private Key	has the meaning given to that expression in the DCCKI Certificate Policy.

Version X 7.0

APPENDIX X

Registration Data Interface Specification

(REGIS)

Contents

DEFINITIONS

In this document, except where the context otherwise requires:

- expressions defined in section A of the Code (Definitions and Interpretation) have the same meaning as is set out in that section; and
- the expressions in the left hand column below shall have the meanings given to them in the right hand column below.

DCC Service Flag	means a flag used to indicate the status recorded by DCC of each MPAN or Supply Meter Point with respect to whether a Smart Metering System is Active, Non-Active or Installed but not Commissioned.
DCC Status File	means the file produced by DCC and transferred to each Network Party's Registration Data Provider detailing the DCC Service Flag of each MPAN or Supply Meter Point registered to that Network Party.
Electricity Registration Data Provider	means a Registration Data Provider appointed by an Electricity Network Party.
Energy Market Data Specification	means the Data Specification which forms part of the REC.
FTP	means file transfer protocol, a standard protocol for transmitting files between computers on a network.
FTPS	means FTP with Transport Layer Security.
Gas Registration Data Provider	means a Registration Data Provider appointed by a Gas Network Party.

Internet Protocol (or IP)	means the commonly used communications protocol enabling the delivery of data packets based on the IP addresses in the packet headers, used in establishing internet communications.
Issuer	has the meaning given to that term in the DCCKI Interface Design Specification.
Network Address Translation	means the standard methodology of remapping one IP address space into another by modifying network address information in Internet Protocol (IP) headers while they are in transit across a traffic routing device.
Policy Enforcement Point (or PEP)	a logical entity that enforces policies for admission control and policy decisions in response to a request for access. It is the logical boundary between the DCC Systems and connecting systems, namely User Systems and RDP Systems. The PEP ensures that: a. the policies in the applicable Code of Connection relevant to the applicable party are being enforced; b. there is appropriate separation of the DCC Systems from the connecting systems of the applicable party; and c. all the connections to the User Systems, RDP Systems, or DCC Systems are compliant with the same applicable Code of Connection .
Response File	means a file produced whilst processing a DCC Status File. For each record in the file being processed, the Response File contains either an acknowledgement that the record has been processed successfully or in the case of a failure in processing the record, the validation errors found.
Supported Version	means the latest version of the Energy Market Data Specification data flow that the DCC supports for use with the Registration Data Interface as listed and as updated from time to time on the Website.
Transport Layer Security (or TLS)	means a protocol that provides for the privacy and integrity of data transferred between communicating applications and their users.

1. INTRODUCTION

Document Purpose

1.1 Pursuant to Section E2 (Registration Data) of the Code, this document is the Registration Data Interface Specification.

2. REGISTRATION DATA INTERFACE

Establishment of the REGIS logical connection

2.1 The DCC shall make the Registration Data Interface available on an Internet Protocol version 4 (IPv4) address range.

2.2 Each Registration Data Provider shall use Network Address Translation to remap their internal Internet Protocol addresses to the DCC provided Internet Protocol addresses at the Registration Data Provider's firewall prior to accessing the Registration Data Interface.

2.3 Each Registration Data Provider shall use Network Address Translation to remap incoming DCC traffic Internet Protocol addresses from the published Internet Protocol addresses at the Registration Data Provider's firewall to the Internet Protocol addresses the Registration Data Provider has reserved within their subnet.

2.4 The DCC shall specify a range of ports and the DCC and each Registration Data Provider shall configure these ports to be open for the FTPS connection.

File Exchange Mechanism

2.5 The Registration Data Interface shall utilise FTPS following the list of recommended tasks for implementing an information exchange stated in NIST SP 800-47 revision 1 Section 3.2.2.

2.6 The DCC and each Registration Data Provider shall implement FTP, in a standard format conforming to the following internet standards as defined in the referenced Request for Comments (RFC) as published by the Internet Engineering Task Force (IETF) and the Internet Society:

(a) RFC 959 - FTP; and

(b) RFC 2228 – FTP security extensions.

2.7 The DCC and each Registration Data Provider shall secure the FTP session using TLS, in a standard format conforming to the following internet standards as defined in the referenced RFC as published by the IETF and the Internet Society:

(a) RFC 4217 - Securing FTP with TLS

2.8 In accordance with RFC 4217:

(a) each Registration Data Provider shall populate the "USER command" (as defined in RFC 4217) with the RDP Signifier issued to it by the Panel, in lower case; and

(b) the DCC shall populate the "USER command" with the Party Signifier issued to it by the Panel, in lower case.

2.9 The DCC and each Registration Data Provider shall ensure the session Transport Layer Security is achieved utilising:

(a) the cipher suite TLS_RSA_WITH_AES_128_GCM_SHA256 as catalogued and further defined by the Internet Assigned Numbers Authority within the Cipher Suite Registry; and

(b) DCCKI Certificates for mutual authentication.

2.10 The DCC and each Registration Data Provider shall ensure that the FTPS session is routed via the DCC's Policy Enforcement Point and the Policy Enforcement Point used by the Registration Data Provider.

2.11 When sending a DCC Status File, the DCC shall follow steps (a) to (d) below, and when receiving a DCC Status File each Registration Data Provider shall follow steps (e) to (K) below:

(a) structure data files provided under Section E2.4 of the Code, in accordance with the structures defined in clause 3.9 of this document;

(b) Digitally Sign the file in accordance with clause 2.12 of this document;

(c) connect to the recipient's FTPS server in accordance with clauses 2.7 to 2.9 of this document using a DCC Gateway Connection;

(d) initiate the transfer of the file to the relevant delivery directory on the recipient's FTPS server utilising FTP push mechanisms for all file exchanges;

(e) authenticate the source of the file through verifying that the file has been Digitally Signed in accordance with clause 2.12 of this document, and validate the file structure against the structure as defined in clause 3.9 of this document;

(f) raise an Incident in accordance with the Incident Management Policy, where the recipient is unable to authenticate the file pursuant to clause 2.16 of this document;

(g) in the case of Electricity Registration Data Providers only, raise an Incident in accordance with the Incident Management Policy, where the Electricity Registration Data Provider is unable to confirm that the file conforms with clause 3.9 of this document;

(h) in the case of Registration Data Providers only, generate a Response File as defined in clause 3.10(a) or 3.13(g) of this document, where the Registration Data Provider is unable to validate the file structure pursuant to clauses 3.11 or 3.14 of this document. The Registration Data Provider shall send the Response File to the DCC using the steps outlined in clauses 2.11(b) to (d) immediately above and on receipt of the Response File containing validation errors the DCC shall raise an Incident as defined in the Incident Management Policy;

(i) process each record within the file and perform record level validation, where the Registration Data Provider or DCC is able to successfully authenticate and validate the file pursuant to clause 2.11(e) of this document;

(j) in the case of Registration Data Providers only, generate a Response File as defined in clauses 3.10(a) and 3.13(g) of this document, where the Registration Data Provider is unable to successfully validate and process each record within the file pursuant to clause 2.11(i) of this document. The Registration Data Provider shall send the Response File to the DCC using the steps outlined in clauses 2.11(b) to (d) and on receipt of the Response File containing validation errors the DCC shall raise an Incident in accordance with the Incident Management Policy; and

(k) in the case of the DCC only, raise an Incident in accordance with the Incident Management Policy, where the DCC is unable to successfully validate and process each record within the file pursuant to clause 2.11(i) of this document.

Security Requirements

2.12 The DCC shall Digitally Sign each file sent via the Registration Data Interface with a Private Key.

2.13 The DCC shall ensure that the Digital Signature shall:

a) use, as the digital signature technique, Elliptic Curve Digital Signature Algorithm (ECDSA) (as specified in Federal Information Processing Standards Publications (FIPS PUB) 186-4) in combination with the curve P-256 (as specified in FIPS PUB 186-4 at Section D.1.2.3) and SHA-256 as the hash function;

b) be applied to the entirety of the file including header and trailer; and

c) be converted to Base64 and appended within the file itself to the trailer with a preceding "," separator.

2.14 Prior to Digitally Signing each file, the DCC shall append to the trailer of the file the Issuer, which shall be URL encoded (as specified in the IETF RFC 2253), and serial number of the SMKI Organisation Certificate with preceding "," separators.

2.15 Each Registration Data Provider may use the organisation identifier in the header of the file and the Issuer and serial number in the trailer of the file to retrieve the appropriate public key.

2.16 Each Registration Data Provider shall Check Cryptographic Protection on a file using ECDSA (as specified in FIPS PUB 186-4) in combination with the curve P-256 (as specified in FIPS PUB 186-4 at Section D.1.2.3) and SHA-256 as the hash function, and Confirm Validity of the Certificate used to Check Cryptographic Protection.

2.17 Each Registration Data Provider shall ensure that the Digital Signature calculation shall:

(a) be performed on the entire file including header and trailer except the Digital Signature and preceding field separator appended to the trailer;

(b) ensure that all line termination characters read from the file, except any termination characters in the trailer, shall be normalised to 0x0A; and

(c) exclude any line termination characters in the trailer.

2.18 Prior to verifying the Digital Signature, each Registration Data Provider shall ensure that all line termination characters in the file, except the line termination characters in the trailer, shall be normalised to 0x0A.

Interface Error Handling

Data files not being received when expected

2.19 Identification of an Anomalous Event:

(a) in the event of the DCC or a Registration Data Provider identifying an exception to the agreed schedules, either organisation may raise an Incident in accordance with the Incident Management Policy.

2.20 Connection & Transfer Failures:

(a) in the event of connection failures or file transfer failures from the DCC to a Registration Data Provider, the DCC shall attempt to reconnect and/or resend the file on 3 further occasions at 5 minute intervals; and

(b) if the DCC cannot establish a connection with the Registration Data Provider after such number of retries, the DCC shall raise an Incident in accordance with the Incident Management Policy.

2.21 Authentication Failure:

(a) In the event of a transport authentication failure where the DCC is trying to send a DCC Status File to a Registration Data Provider, a transport authentication failure will result in no connection or transmission of Registration Data. In such circumstances, the DCC shall raise an Incident in accordance with the Incident Management Policy.

Data files not conforming to the Registration Interface Specification

2.22 Identification of an Anomalous Event:

(a) The Registration Data Provider shall perform a check of the conformity of files against the agreed standards set out in clause 3 of this Registration Data Interface Specification; or

(b) In the event of either the DCC or a Registration Data Provider being in receipt of a non-conforming file it shall raise an Incident in accordance with the Incident Management Policy.

2.23 Validation Failure:

(a) where a validation failure is identified as a result of a DCC file that has been sent to the Registration Data Provider, the Registration Data Provider shall raise an Incident in accordance with the Incident Management Policy.

2.24 Other Circumstances:

(a) in the event of an Incident arising that is not covered by clauses 2.19 to 2.23 above, a Registration Data Provider shall review its business processes; and

(b) following compliance with clause 2.23(a) above, and in the event a Registration Data Provider has reasonable grounds to expect the issue to reside within the DCC, the Registration Data Provider shall raise an Incident in accordance with the Incident Management Policy.

Notification of Delays

2.25 In the event that the DCC has a planned or unplanned delay to a DCC Status File transfer, the DCC shall raise an Incident in accordance with the Incident Management Policy.

3. <u>INTERFACE FILES</u>

General Obligations

3.1 The DCC shall maintain a separate unique reference number for each Network Party that it shall apply to all files corresponding to that Network Party that it sends through the Registration Data Interface to that Network Party's Registration Data Provider.

3.2 In the event that a file is suspected of being lost, each Registration Data Provider may raise an Incident in accordance with the Incident Management Policy.

3.3 Each Electricity Registration Data Provider shall, pursuant to clause 2.11(j), reject a record with a DCC Service Flag 'effective from date' for a Smart Metering System that is earlier than the DCC Service Flag 'effective from date' previously provided by the DCC for that Smart Metering System.

3.4 Each Gas Registration Data Provider shall detect duplicate files and where detected shall not process duplicate files.

3.5 Each Gas Registration Data Provider shall process files in the order they are received.

3.6 Each Registration Data Provider and the DCC shall not use file compression on files transferred through the Registration Data Interface.

3.7 The DCC shall provide any DCC Status Files utilising the FTPS connection or via an alternative means as agreed between the DCC and the Gas Registration Data Provider or Electricity Registration Data Provider to whom the file is being sent, (provided that any such alternative means must incorporate the use of security controls that are at least as robust as those that apply to the FTPS connection).

Electricity Registration Data File Structure and Data Formats

3.8 The DCC shall use variable length delimited file format for sending files, which meet the following requirements:

(a) fields shall be separated with "|" (ASCII 124) characters

(b) only use ASCII characters;

(c) not exceed the field lengths shown in the flow definitions referenced in clause 3.9 of this document;

(d) values shall not be padded (with leading zeroes or trailing spaces) where less than the maximum field length;

(e) fields shall not be enclosed in double quotes;

(f) no characters shall be entered into fields that are intended to be blank; and

(g) records shall be terminated with a line feed (ASCII 10) character.

3.9 The DCC shall ensure that all files contain header and trailer records that conform to the formats as specified below:

(a) File Header

Data Item	Format	Optionality	Comment
Group Header	CHAR(3)	Mandatory	'ZHV'
File Identifier	CHAR(10)	Mandatory	File identifier - unique within market participant
Data flow and Version Number	CHAR(8)	Mandatory	Dxxxxnnn Consists of 5 char data flow reference followed by 3 char flow version number - where 'n' has a range of 0-9 e.g. 001, 105....
From Market Participant Role Code	CHAR(1)	Mandatory	e.g. Registration systems have value P
From Market Participant Id	CHAR(4)	Mandatory	e.g. DCC has value DCCO
To Market Participant Role Code	CHAR(1)	Mandatory	e.g. DCC has value Z
To Market Participant Id	CHAR(4)	Mandatory	e.g. DCC has value DCCO
File creation timestamp	CHAR(14)	Mandatory	DATETIME (GMT) DCC is using UTC Formatted: YYYYMMDDHHMMSS
Sending Application Id	CHAR(5)	Optional	Application identifier. For possible future use
Receiving Application Id	CHAR(5)	Optional	Application identifier. For possible future use
Broadcast	CHAR(1)	Optional	For possible future use.
Test data flag	CHAR(4)	Optional	Indicates whether or not this file contains test data. All operational (non-test) files shall contain the value OPER

(b) File Trailer

Data Item	Format	Optionality	Comment
Group Name	CHAR(3)	Mandatory	'ZPT'

File identifier	CHAR(10)	Mandatory	File identifier - unique within market participant
Total Group Count	INT (10)	Mandatory	Total number of groups in file excluding header/trailer
Checksum	INT (10)	Optional	Checksum
Flow count	INT (8)	Mandatory	Number of flow instances excluding file header/trailer
File completion timestamp	CHAR(14)	Optional	DATETIME (GMT) DCC is using UTC Formatted: YYYYMMDDHHMMSS

3.10 Each Electricity Registration Data Provider shall provide the following files, which shall conform to the latest Supported Version of the specified data flow structures as defined in the Energy Market Data Specification:

(a) Response File - DCC Service Flag update rejections

To notify the DCC of any data records rejected during processing of a DCC Status File due to validation errors, each Electricity Registration Data Provider shall send a Response File as specified in the Energy Market Data Specification D0351 data flow; and

(b) Response File - DCC Service Flag update acknowledgement

To notify the DCC of successful processing of the DCC Status File, each Electricity Registration Data Provider shall send a Response File as specified in the Energy Market Data Specification D0172 data flow.

3.11 The DCC shall provide the following files to each Electricity Registration Data Provider conforming to the data flow structures as defined in the Energy Market Data Specification:

(a) DCC Status File

To notify Electricity Network Parties of DCC Service Flag updates and the identity of the person that the DCC believes to be registered in relation to an MPAN as set out in Section E2.4 of the Code, the DCC shall send a DCC Status File as specified in the Energy Market Data Specification D0350 data flow.

3.12 Clause 3.11 constitutes the data that is to be provided by the DCC to Registration Data Providers under Section E2.4 (a) of the Code.

Gas Registration Data File Structure and Data Formats

3.13 The DCC shall use comma separated file format for sending files to Registration Data Providers of Gas Transporters, and each shall ensure that all of the files that it sends meet the following requirements:

(a) fields shall be comma-separated;

(b) only use ASCII characters;

(c) do not exceed the field lengths shown below at clause 3.28 of this document and exclude any opening and closing double quotation marks or comma separators;

(d) values shall not be padded where less than the maximum field length;

(e) text fields shall be enclosed with opening and closing double quotation marks, but no quotation marks shall be used in date and numeric fields; and

(f) blank fields shall not contain characters other than opening and closing double quotation marks for text fields.

3.14 Each Gas Registration Data Provider shall employ the file naming convention described below, ensuring that each file sent through the DCC Gateway Connection has a unique name. Within the names shown in clauses (a) and (b) below: 'PN' indicates that the files are production (will be 'TN' for test); nnnnnn is the sequence number of the file in question; and xxx is the file type (ERR, FRJ or DXR) as detailed in clause 3.16:

(a) Daily DCC Status Files:
DCC01.PNnnnnnn.DXI

(b) Response Files from Daily DCC Status File processing will be:
XOS01.PNnnnnnn.xxx

(c) Response File - DCC Service Flag update responses

Following the processing of the DCC Status File (file format described in clause 3.29(a) of this document) each Gas Registration Data Provider shall provide a Response File indicating whether each of the DCC Service Flag update records (record reference 'E45') was accepted or rejected. For each E45 record in the incoming "DXI" DCC Status File there will be a corresponding E46 record (as described immediately below) in the "DXR" Response File. If the E45 record is processed successfully, the outcome code in the E46 record will be "AC" and if unsuccessful the outcome code is "RJ".

Where the outcome is "RJ" the rejection reason will be notified to the DCC through an S72 record or records directly following the E46.

(i) The format of an E46 record is as follows:

Field Name	Optionality	Type	Length	Description
Transaction Type	Mandatory	Text	3	Value: E46
Outcome Code	Mandatory	Text	2	Details whether the request has been accepted or rejected. AC – Accepted RJ – Rejected.
Meter Point Reference	Mandatory	Number	10	
DCC Service Flag	Mandatory	Text	1	Service flag provided by the DCC. The allowable values are: • A – Active • N – Non-Active • I – InstalledNotCommissioned
DCC Service Effective From Date	Mandatory	Date	8	The date the DCC Service Flag (provided above) is effective from. Format : YYYYMMDD

Service Flag	Description
Active	DCC Service Flag 'A' requires at least one of the associated Smart Meters at an SMS to have the 'Commissioned' Device status in the SMI.

Non-Active	DCC Service Flag 'N' indicates that an SMS is not associated with a Device with an 'InstalledNotCommissioned' or 'Commissioned' Device status, but has been previously.
InstalledNotCommissioned	DCC Service Flag 'I' requires all the associated Smart Meters at an SMS to have the 'InstalledNotCommissioned' Device status in the SMI.

(ii) The format of an S72 record is as follows:

Field Name	**Optionality**	**Type**	**Length**	**Description**
Transaction Type	Mandatory	Text	3	Value: S72
Rejection Code	Mandatory	Text	8	The unique reference number identifying the reason for the validation failure. One of the following two values: 'MPO00001' Supply Meter Point does not exist 'DCC00001' DCC Service Flag value is not recognised

3.15 The DCC shall provide files to each Gas Registration Data Provider conforming to the following data flow structure:

(a) DCC Status File

To notify each Gas Registration Data Provider of DCC Service Flag updates the DCC shall send a single DCC Status File (Ref DXI) that shall consist of a single data record per update (Ref. E45). The format of an E45 record is as follows:

Field Name	**Optionality**	**Type**	**Length**	**Description**	**SEC reference**
Transaction Type	Mandatory	Text	3	Value: E45	Not applicable
Meter Point Reference	Mandatory	Number	10		Section E2.4 (b)
DCC Service Flag	Mandatory	Text	1	Service flag provided by the DCC. The allowable flags are: • A – Active • N – Non-Active • I – InstalledNotCommissioned	Section E2.4(b)
DCC Service Effective From Date	Mandatory	Date	8	The date the DCC Service Flag (provided above) is effective from. Format : YYYYMMDD	Section E2.4 (b)

3.16 Each Gas Registration Data Provider shall create and send the Response Files as defined in clause 3.16 (a) and (b) below, in response to failures in validation of the DCC Status File. On receipt of the Response File DCC shall raise an Incident as defined in the Data Incident Management Policy.

(a) Record level format failure Response File

To record any record level format validation errors found in processing the DCC Status File, the Gas Registration Data Provider shall create a Response File with header and trailer as defined in clause 3.14 of this document and one or more record level error records as detailed below. The file name will be as defined in clause 3.14(b) of this document with suffix 'ERR'.

Field Name	Optionality	Type	Length	Description
Transaction Type	Mandatory	Text	3	Value: E01
Rejection Code	Mandatory	Text	8	The unique reference number identifying the reason for the validation failure as defined in the Error Code under clause 3.30(c)
File Reference	Mandatory	Number	10	The unique reference number of the file that was received and processed.
Rejection Description	Mandatory	Text	250	Description of the error found and which record/field it occurred as defined in the Rejection Reason under clause 3.30(c).

(b) Response File - File level rejection

To record any file level format validation errors found in processing the DCC Status File, the Registration Data Provider shall create a Response File with header and trailer as defined in clause 3.26 of this document and the file name will be as defined in clause 3.24(d) of this document with suffix 'FRJ'. File level validation failures will be contained within a single file and will consist of 2 different types of data record per file – Rejected File (record reference S71) and Rejection Details (record reference S72). There will be one S71 record followed by one or more S72 records.

(i) The format of an S71 record is as follows:

Field Name	Optionality	Type	Length	Description
Transaction Type	Mandatory	Text	3	Value: S71
File Reference	Mandatory	Text	30	The unique reference number of the file that was received and processed.

(ii) The format of an S72 record is as follows:

Field Name	Optionality	Type	Length	Description
Transaction Type	Mandatory	Text	3	Value: S72

Rejection Code	Mandatory	Text	8	The unique reference number identifying the reason for the validation failure as defined in the Error Code under clause 3.30(d)

(c) Record level - Error codes

Error Code	
CSV00010	Transaction type not recognized - <*Record identifier*>
CSV00011	Invalid character - <*Record identifier*>, <*Field number*>
CSV00012	Invalid numeric field , <*Record identifier*>, <*Field number*>
CSV00013	Premature end of record - <*Record identifier*>
CSV00014	Invalid record termination - <*Record identifier*>
CSV00015	Invalid text field - <*Record identifier*>, <*Field number*>
CSV00019	Record too short - <*Record identifier*>
CSV00020	Mandatory field expected - <*Record identifier*>, <*Field number*>
CSV00021	Invalid Date/Time field - <*Record identifier*>, <*Field number*>
CHK00036	Mandatory record not supplied - <*Record identifier*>

(d) File level - Error codes

FIL00013	Organisation ID on header cannot be found
FIL00014	Organisation ID on the header does not match the sender's ID
FIL00015	File type on the header is not the same as that in file name
FIL00016	Generation number on the header is not the same as that in file name
FIL00017	A file has previously been received & processed with this generation number
FIL00018	A count of detail records in the file does not match that held on the trailer
FIL00019	Invalid record type found

Version Y 3.0

APPENDIX Y

Registration Data Interface Code of Connection

(REGICoCo)

DEFINITIONS

In this document, except where the context otherwise requires:

- expressions defined in Section A of the Code (Definitions and Interpretation) have the same meaning as is set out in that Section;
- the expressions in the left hand column below shall have the meanings given to them in the right hand column below; and
- any expressions not defined here or in Section A of the Code have the meaning given to them in the Registration Data Interface Specification.

Security Patch	means a software change intended to address a particular vulnerability or weakness in the security of a system.

1. REGISTRATION DATA INTERFACE CODE OF CONNECTION

1.1 These provisions apply to the DCC and any Registration Data Provider seeking to receive communications via the Registration Data Interface.

General Obligations

1.2 The DCC and each Registration Data Provider shall inform each other of the contact details of one or more persons working for their respective organisations for the purposes of managing arrangements associated with the use of the Registration Data Interface. The following information shall be provided in relation to each such person (and subsequently kept up to date by the providing organisation):

(a) contact name;

(b) contact email;

(c) contact telephone number; and

(d) contact address.

and any other contact details as may be reasonably required by the DCC or the Registration Data Provider from time to time.

Restrictions on the use of DCC Gateway Connections

1.3 The DCC shall use a DCC Gateway Connection for the purpose of sending data to the Registration Data Provider pursuant to Section E2 of the Code, except where an alternative means of transfer has been agreed pursuant to clause 3.7 of the Registration Data Interface Specification.

Establishment of Transport Layer Security

1.4 The DCC and each Registration Data Provider:

(a) shall establish a TLS session to secure the transport layer connection to the Registration Data Provider's FTPS server and the DCC's FTPS server respectively and shall do so in accordance with the Registration Data Interface Specification;

(b) shall use a DCCKI Infrastructure Certificate to establish the TLS session; and

(c) in the case of a Registration Data Provider only, may obtain a DCCKI Infrastructure Certificate in accordance with the DCCKI RAPP.

DCC Status Files

1.5 The DCC shall produce a DCC Status File showing the changes to the DCC Service Flag for each MPAN or Supply Meter Point that occurred since the last update, provided that where no such changes have occurred, the DCC Status File shall record zero changes.

1.6 The DCC shall send a DCC Status File by 18:00 hours every day. In the case of Gas Smart Metering Systems, the DCC shall send one DCC Status File per Registration Data Provider. In the case of Electricity Smart Metering Systems, the DCC shall send one DCC Status File per Electricity Network Party.

Technical Infrastructure

1.7 Each Registration Data Provider shall provide and configure its own FTPS servers for use in receipt of data from the DCC as set out in Section E2.4 and shall be responsible for operation and maintenance of its FTPS platform used to receive files from the DCC.

1.8 Each Registration Data Provider and the DCC shall inform each other of information relating to its FTPS servers that is reasonably required by the DCC and each Registration Data Provider in relation to any DCC Gateway Connection that it is using to access the Registration Data Interface.

1.9 The DCC shall ensure that the URLs and/or the IP addresses of the Registration Data Interface remain constant.

Security Obligations

1.10 Each Registration Data Provider shall test the installation of Security Patches to be applied to its RDP Systems prior to their application.

1.11 Prior to using the Registration Data Interface, each Registration Data Provider shall provide a report to the DCC that details the following:

(a) the scope of its RDP Systems;

(b) the number of connections between its RDP Systems and any System that does not form part of the RDP Systems; and

(c) the means by which the Registration Data Provider has achieved Separation between its RDP Systems and each other System to which they connect.

and;
thereafter, the Registration Data Provider shall ensure that the DCC is provided with a revised report whenever there is a change to the information in its previous report.

1.12 Where, based upon the report provided by the Registration Data Provider in clause 1.24 of this document the DCC considers that the Registration Data Provider has not adequately Separated its RDP Systems from other systems to which those RDP Systems connect, then to the extent that the failure to adequately Separate poses a threat of Compromise to DCC's Systems, the DCC shall notify the Registration Data Provider, the relevant Network Party, and the Panel and provide an associated explanation.

Version Z 8.0

APPENDIX Z

CPL Requirements Document

1. Overview

1.1 This Appendix supplements Section F2 (Central Products List).

2. Central Products List Contents

2.1 The Panel shall ensure that the Central Products List identifies each Device Model by Physical Device Type, and lists the following matters in respect of each Device Model:

(a) Manufacturer and model;

(b) hardware version;

(c) firmware version;

(d) for SMETS2+ Device Models, the version of the SMETS or CHTS (as applicable) and (in each case) the GBCS version for which the Device Model has one or more Assurance Certificates;

(e) for SMETS1 Device Models, Version 1.2 of SMETS;

(f) for SMETS2+ Device Models, the identification numbers for each of the Device Model's Assurance Certificates (including the version of the relevant standard against which each Assurance Certificate was issued);

(g) where the Device Model is required to have an associated CPA Certificate, the expiry or renewal date of the Device Model's CPA Certificate and the associated version of the Security Characteristics (as defined in the relevant Technical Specification);

(h) where there is an associated Manufacturer Image:

(i) the relevant identity of the person who created the Manufacturer Image;

(ii) a descriptor of the Manufacturer Image;

(iii) the Hash of the Manufacturer Image (to be provided pursuant to Clause 4); and

(i) Zigbee band, which is a mandatory field.

3. Addition of Device Models to the List

3.1 For SMETS2+ Device Models, the Panel shall only add Device Models to the Central Products List once the Panel has received all the Assurance Certificates required (under the Technical Specifications) to be obtained in respect of Device Models of the relevant Physical Device Type (which Assurance Certificates may be provided to the Panel by a Party or any other person).

3.2 For SMETS1 Device Models, the Panel shall only add a Device Model to the Central Products List once the Panel has received a notification from the DCC or, subject to Clause 3.5, from a Supplier Party. Clauses 3.3 to 3.13 (inclusive) set out the process for adding SMETS1 Device Models to the Central Products List.

3.3 The DCC shall only send a notification to the Panel in respect of a SMETS1 Device Model (as referred to in Clause 3.2) once the Device Model has been included as part of at least one entry on the SMETS1 Eligible Products Combinations list.

3.4 A Supplier Party may only send a notification to the Panel in respect of a SMETS1 Device Model (as referred to in Clause 3.2) if:

(a) that SMETS1 Device Model has not been included as part of at least one entry on the SMETS1 Eligible Product Combinations list; and

(b) that Supplier Party reasonably believes that the addition of the SMETS1 Device Model to the Central Products List is required in order to facilitate the urgent resolution of a material security vulnerability relating to Commissioned Devices for which it is the Responsible Supplier.

3.5 As soon as reasonably practicable after sending a notification to the Panel in accordance with Clause 3.2, the relevant Supplier Party shall notify the DCC via the Notification Interface that it has sent such a notification to the Panel and, in doing so, shall inform the DCC of the Device Model notified to the Panel.

3.6 The Panel shall only accept and process a notification from a Supplier Party under Clause 3.2 if the notification has been made in accordance with the requirements of the Supplier Party CPL Notification Procedures and where the Panel has successfully confirmed that the notification was from a Supplier Party and has not been modified since its creation.

3.7 For the purposes of Clause 3.6, the Supplier Party CPL Notification Procedures are procedures that provide for a Device Model to be notified to the Panel by a Supplier Party in a manner that allows the Panel to confirm that:

(a) any such notification has originated from a Supplier Party; and

(b) any such notification from a Supplier Party has not been modified since its creation.

3.8 The Panel shall develop the Supplier Party CPL Notification Procedures and any subsequent modification to them in consultation with the Security Sub-Committee and publish the Supplier Party CPL Notification Procedures on the Website.

3.9 Where the DCC has received a notification via the Notification Interface from a Supplier Party pursuant to Clause 3.5, the DCC shall, as soon as reasonably practical after uploading into the DCC Systems a revised version of the Central Products List that additionally includes the Device Model notified to the Panel by the Supplier Party, inform that Supplier Party via the Notification Interface that the upload has taken place.

3.10 For the purposes of Clauses 3.5 and 3.9, the Notification Interface is an appropriately secure interface, the identity of which the DCC shall communicate to Supplier Parties, for the purposes of making the notifications between Supplier Parties and the DCC referred to in those Clauses.

3.11 After the addition of a Non-EPCL Device Model to the Central Products List, the Supplier Party that notified the Non-EPCL Device Model to the Panel shall take all reasonable steps to ensure that each Device Model Combination:

(a) of which any Commissioned Device of that Non-EPCL Device Model forms part; and

(b) for which Commissioned Device it is the Responsible Supplier, is added to the SMETS1 Eligible Product Combinations List as soon as reasonably practicable.

3.12 After the Commissioning of a Device that is of a Non-EPCL Device Model, the Responsible Supplier for that Device shall take all reasonable steps to ensure that that the Device Model Combination of which that Device forms part is added to the SMETS1 Eligible Product Combinations List as soon as reasonably practicable.

3.13 Where a PPMID of a particular type is capable of forming part of either a SMETS1 Smart Metering System or a SMETS2+ Smart Metering System, any Device Model added to the Central Products List shall:

(a) insofar as it relates to PPMIDs of that type forming part of SMETS2+ Smart Metering Systems, be the Manufacturer of the PPMID, its model, its hardware version and its firmware version; and

(b) insofar as it relates to PPMIDs of that type forming part of SMETS1 Smart Metering Systems, be the Manufacturer of the PPMID, its model, its hardware version and a value representing its firmware version that is different to the firmware version of the PPMID of that type that forms part of a SMETS2+ Smart Metering System.

4. Association of Hashes with Device Models on the CPL

4.1 Where the DCC, a Supplier Party or a Manufacturer which is a Party wishes the Panel to associate the Hash of a Manufacturer Image with a Device Model on the Central Products List, that Party shall provide the Hash and the identity of the person who created the Manufacturer Image in a communication to the Panel which has been Digitally Signed by the person who created the Manufacturer Image in a manner that reasonably enables the Panel to check that the communication originates from the person who created the Manufacturer Image.

4.2 The Panel may specify the format which the communication referred to in Clause 4.1 must take (in which case Parties sending such communications must use such format). The Panel shall notify the relevant Parties of any such required format and of any changes to such required format that the Panel may make from time to time.

4.3 The Panel shall only associate a Hash provided under Clause 4.1 with a Device Model on the Central Products List where:

(a) the Panel has successfully confirmed that the Digital Signature referred to in Clause 4.1 is that of the person who created the Manufacturer Image (validated as necessary by reference to a trusted party);

(b) there is no Hash currently associated with the Device Model; provided that, if there is a Hash currently associated with the Device Model, the Panel shall investigate the matter with the relevant Parties to identify whether it is appropriate to replace the associated Hash (and shall, where it is appropriate to do so, update the Central Products List accordingly); and

(c) if the Device Model is a SMETS1 Device Model, the communication to the Panel referred to in Clause 4.1 is from the DCC.

5. Adding Device Models to CPA Certificates

5.1 An existing CPA Certificate for a Device Model may allow one or more additional Device Models to be added under that existing CPA Certificate, provided that any additional Device Model differs from the Device Model for which the CPA Certificate was originally issued only by virtue of having different versions of hardware and/or firmware that do not have a significant impact on the security functions of the Device Model (as set out in the CPA Assurance Maintenance Plan). Where this is the case, the following persons may notify the Panel of one or more additional Device Models to be added to the CPA Certificate:

(a) the DCC for Communications Hubs; or

(b) a Supplier Party or a Manufacturer which is a Party for Device Models of all other Physical Device Types.

5.2 Where the DCC, a Supplier Party or a Manufacturer which is a Party notifies the Panel of an additional Device Model pursuant to Clause 5.1, the DCC, Supplier Party or Manufacturer shall:

(a) only do so in accordance with the terms of the relevant CPA Assurance Maintenance Plan; and

(b) retain evidence that it has acted in accordance with the terms of the relevant CPA Assurance Maintenance Plan, such evidence to be provided to the Panel or the Authority on request.

5.3 The Panel shall not be required to check whether the DCC, a Supplier Party or Manufacturer (as applicable) is entitled to add a Device Model under the terms of the CPA Certificate and the CPA Assurance Maintenance Plan (as described in Clause 5.1).

5.4 [NOT IN USE]

6. Removal of Device Models from the List

6.1 Where an Assurance Certificate for a Device Model which was issued by the ZigBee Alliance or the DLMS User Association is withdrawn or cancelled by the ZigBee Alliance or the DLMS User Association (as applicable), then the Panel shall remove that Device Model from the Central Products List.

6.2 Where a CPA Certificate for a Device Model expires or is not renewed or is withdrawn or cancelled by NCSC or a Trial Device Certificate for a Trial Device Model expires or is withdrawn or cancelled by the Security Sub-Committee, then the Security Sub-Committee shall determine whether the Device Model is to be removed from the Central Products List, and the Panel shall remove the Device Model (or not) as determined by the Security Sub-Committee. In reaching such a determination, the Security Sub-Committee:

(a) shall consider the security implications of such circumstances, and weigh them against the consequences for Energy Consumers of Devices of the relevant Device Model being Suspended as a result of removing the Device Model from the Central Products List;

(b) shall take into account any relevant information provided to it by NCSC concerning the risks associated with the cancellation, withdrawal or expiry without renewal of the CPA Certificate;

(c) may determine, whether or not the Device Model is to be removed from the Central Product List, that a CPA Certificate Remedial Plan or a Trial Device Remedial Plan (as relevant) is to be imposed (for SMETS2+ Communications Hubs) on the DCC or (for all other Device Models) on the Import Suppliers (for Devices of that Device Model forming part of a Smart Metering System for which they are the Import Supplier) and/or the Gas Suppliers (for Devices of that Device Model forming part of a Smart Metering System for which they are the Gas Supplier); and

(d) shall reach a determination as soon as reasonably practicable taking into account the seriousness of the potential security consequences.

6.3 Where the Security Sub-Committee determines under Clause 6.2 that a CPA Certificate Remedial Plan or a Trial Device Remedial Plan (as relevant) is to be imposed on one or more Parties, then the Security Sub-Committee shall notify those Parties and each of those Parties shall:

(a) (within such period as the Security Sub-Committee may require) propose a plan to the Security Sub-Committee setting out how the Party intends to remedy the security issue or issues that have resulted in or arise from the cancellation, withdrawal or expiry without renewal of the CPA Certificate or Trial Device Certificate, and within what time period;

(b) (within such period as the Security Sub-Committee may require) take into account any and all comments on the proposed plan raised by the Security Sub- Committee, and obtain the Security Sub-Committee's approval of the plan (the approved plan for each such Party, as modified from time to time with the approval of the Security Sub-Committee, being that Party's "**CPA Certificate Remedial Plan**" or, in the case of a Trial Device Certificate, its "**Trial Device Remedial Plan**");

(c) comply in all material respects with the CPA Certificate Remedial Plan or Trial Device Remedial Plan (as relevant); and

(d) (where requested by the Security Sub-Committee) report to the Security Sub-Committee on progress in respect of the CPA Certificate Remedial Plan or Trial Device Remedial Plan (as relevant).

6.4 Where the Security Sub-Committee initially determines under Clause 6.2 that a CPA Certificate Remedial Plan or Trial Device Remedial Plan (as relevant) is to be imposed as an alternative to removing a Device Model from the Central Products List, then the Security Sub-Committee may at any time determine that the Device Model in question is to be removed from the Central Products List, in which case the Panel shall remove the Device Model from the Central Products List.

6.5 For the purposes of Section M8.1(g) (Events of Default), the obligations of a Party under Clause 6.3 are material obligations. Accordingly, failure by a Party to gain approval for, or failure by a Party to comply in all material respects with, a CPA Certificate Remedial Plan shall be an Event of Default if not remedied within 20 Working Days after notice from the Security Sub-Committee requiring remedy.

6.6 The DCC, each Supplier Party and each Manufacturer which is a Party shall provide such relevant information as the Security Sub-Committee may reasonably request to assist it in reaching a determination under Clause 6.2 or 6.4.

6.7 The DCC, each Supplier Party and each Manufacturer which is a Party shall notify the Panel of any withdrawal, expiry or cancellation of an Assurance Certificate of which the DCC, Supplier Party or Manufacturer becomes aware. Where removal occurs as a result of the withdrawal, expiry or cancellation of an Assurance Certificate, the Panel shall only remove a Device Model from the Central Products List after the Panel has confirmed with the relevant Assurance Certification Body that the Assurance Certificate for that Device Model has expired or has been withdrawn or cancelled (and no new Assurance Certificate has been provided to the Panel under Clause 3).

6.8 The Panel may also remove a SMETS1 Device Model from the Central Products List where either:

(a) the Security Sub Committee advises that the Device Model should be removed from the Central Products List; or

(b) it is determined by the Authority or by the Panel under Section F3 (Panel Dispute Resolution Role) that Devices of the relevant Device Model are not compliant with SMETS1 (either on their own or in combination with Devices of other Device Models listed on the Central Products List).

6.9 The Panel may reinstate to the Central Products List a SMETS1 Device Model that it has removed pursuant to Clause 6.8; provided that the Panel may only reinstate a Device Model that has been removed pursuant to Clause 6.2A(b) where it determines that the issue that gave rise to the removal of the Device Model has been rectified.

6.10 For the purposes of this Code, a Communications Hub Function or a Gas Proxy Function shall be considered to be on (or not on) the Central Products List if the Communications Hub of which it forms part is on (or not on) the Central Products List.

6.11 The Panel may provide for the removal of a Device Model from the Central Products List by marking that Device Model as 'removed'. All references in this Code to the removal of a Device Model from the Central Products List (and similar expressions) shall be interpreted accordingly.

7. Digital Signatures on CPL

7.1 When providing an updated Central Products List (or extract of it) to the DCC, the Panel shall provide a copy of the Central Products List (or of that extract) that is Digitally Signed so as to reasonably enable the DCC to check that the updates to the Central Product List originate from the Panel.

7.2 The DCC shall, before using and relying upon the Central Products List received by the DCC from the Panel, first confirm that the Digital Signature referred to in Clause 7.1 is that of the Panel (validated as necessary by reference to a trusted party).

7.3 Following receipt by the DCC of an updated Central Products List from the Panel, the DCC shall take all reasonable steps to establish whether the update included the removal of one or more Device Models from the Central Products List. Where the DCC establishes that an update did include the removal of one or more Device Models from the Central Products List, then:

(a) the DCC shall take all reasonable steps to confirm that it was the intention of the Panel to remove such Device Models from the Central Products List; and

(b) where the DCC reasonably believes that it was not the intention of the Panel to remove such Device Models from the Central Products List, the DCC shall notify the Panel that this is the case and (notwithstanding Section F2.9) shall ignore the updated Central Products List.

Version AA 4.0

Appendix AA

Threshold Anomaly Detection Procedures

Contents

DEFINITIONS

In this document, except where the context otherwise requires:

- expressions defined in section A of the Code (Definitions and Interpretation) have the same meaning as is set out in that section; and
- the expressions in the left hand column below shall have the meanings given to them in the right hand column below.

Anomaly Detection Thresholds File	means a CSV file submitted by a User for the purposes of notification of ADT and Warning Thresholds to be applied by the DCC.
Authorised Responsible Officer (ARO)	means an individual that has successfully completed the process for becoming an ARO on behalf of a Party, RDP, SECCo or a DCC Service Provider in accordance with the SMKI RAPP.
Comma Separated Values (CSV)	means a tabular set of data records in text format in which the data fields within each data record are delimited using commas, and where data fields are not

	enclosed with opening and closing double quotation marks.
DCC Service Management System (DSMS)	means the Service Desk system used to manage Incidents and Service Management Service Requests.
Fast-Track Notification	means submission from a User to the DCC of an Anomaly Detection Thresholds File that is submitted with the intention of being applied in shorter timescales than standard processing timescales, where such timescales are set out in clause 3 of this document.
File Signing Certificate	means an IKI Certificate issued to a Party in accordance with the SMKI RAPP and associated with a Private Key that is used for the purposes of Digital Signing of CSV files.
Functional Component	has the meaning ascribed to this term in the Self Service Interface Access Control Specification.
Quarantined Communications Action File	means a CSV file submitted by a User for the purposes of notifying the DCC of the actions to be taken by DCC in respect of quarantined communications.
Quarantined Communications Report File	means a CSV file issued by the DCC to notify a User that communications have been quarantined.
Senior Responsible Officer (SRO)	means an individual that has successfully completed the process for becoming an SRO on behalf of a Party, RDP, SECCo or a DCC Service Provider in accordance with the SMKI RAPP.
Service Management Service Request (SMSR)	means the request raised by the User to facilitate management of a Service Desk call.
Warning Threshold	in respect of a User, a number of communications within a period of time which, if exceeded, will result in the DCC notifying the User. Where both that number and the period of time are set by the User.

1. Introduction

1.1 The Threshold Anomaly Detection Procedures (TADP) document makes provision for such matters as are described in Section G6.1 and G6.4 (b) (i) of the Code, and provides further processes and detail required to facilitate those matters.

2. DCC Anomaly Detection Threshold Guidance

2.1 Pursuant to Section G6.4 (b) of the Code, each User shall take into account any guidance issued by the DCC as to the appropriate level for their Anomaly Detection Thresholds (ADTs) giving regard to their Service Request forecast and expected pattern of demand for each Service Request.

2.2 DCC shall:

(a) provide guidance to support Users in setting appropriate ADT and Warning Thresholds;

(b) provide a template for the User to provide its ADT and Warning Thresholds in the format set out in clause 6.3 of this document;

(c) provide guidance to support Users in submitting ADT submissions to the DCC via the DCC's secure delivery method of choice; and

(d) provide the guidance and template referred to above via the Self Service Interface (SSI).

3. Notification of Anomaly Detection Thresholds

User and DCC Responsibilities: ADT submissions

3.1 Prior to sending the DCC any Anomaly Detection Thresholds File, the User shall raise a DCC Service Management Service Request (SMSR) via the SSI to obtain a reference number for use in its submission to DCC, where such reference number will be generated by the SSI automatically.

3.2 Each User shall use reasonable steps to organise its business processes in such a manner that obviates the need for it to rely on the use of Fast-Track Notifications.

3.3 Where a User wishes to submit a Fast-Track Notification it shall, prior to doing so, contact the DCC and provide a justification for why it is necessary for them to do so.

3.4 A User shall, in each User Role in relation to which it is required (or elects) to set ADTs, provide an Anomaly Detection Thresholds File to the DCC via the DCC's secure delivery method of choice (as from time to time specified on the SSI). The User shall include in such submission:

(a) the SMSR reference number in the subject line of the submission; and

(b) the Anomaly Detection Thresholds File (of the form set out in clause 6.3 of this document), Digitally Signed by a Private Key associated with a File Signing Certificate and provided to an Authorised Responsible Officer (ARO) in accordance with the SMKI RAPP.

3.5 The User shall update the SMSR corresponding to the Anomaly Detection Thresholds File submission on the SSI. On receipt of an SMSR and accompanying Anomaly Detection Thresholds File, the DCC shall:

(a) Check Cryptographic Protection applied to the CSV file, Confirm Validity of the Certificate used to Check Cryptographic Protection for the CSV file;

(b) confirm that the sequence number contained within the Anomaly Detection Thresholds File is greater than the sequence number contained within any previous Anomaly Detection Thresholds File that the

DCC has successfully validated and processed in relation to the User ID specified within that Anomaly Detection Thresholds File;

(c) check that the format of the Anomaly Detection Thresholds File is correct;

(d) confirm that the Anomaly Detection Thresholds File does not contain two or more entries which specify both the same value for the Service Reference Variant and the same value for the Time Period Applicable; and

(e) for Fast-Track Notifications, assess whether the justification provided is valid.

3.6 Following the checks above the DCC shall verify that the ADT and Warning Threshold values provided are consistent with guidance issued by DCC. Where the DCC considers this not to be the case it shall contact a Senior Responsible Officer (SRO) acting on behalf of the User, by telephone using the contact details held by the DCC. The DCC shall request confirmation from the SRO as to whether the submitted Anomaly Detection Thresholds File should be applied. The SRO shall either:

(a) provide confirmation to the DCC to apply the ADT and Warning Thresholds that it has submitted in which case the DCC shall apply the ADT and Warning Thresholds included within the Anomaly Detection Thresholds File and close the relevant SMSR; or

(b) resubmit Anomaly Detection Thresholds File having had further regard to the guidance.

3.7 The DCC shall validate and process Anomaly Detection Thresholds File submissions and shall either apply the ADT and Warning Thresholds in accordance with the manner as is set out in Clause 3.8 or in the event that any of the checks set out in Clause 3.5 (a) to (e) above are not successfully applied, reject the submission, in accordance with the timescales set out immediately below:

(a) for a notification of an Anomaly Detection Thresholds File that is not a Fast-Track Notification, within 72 hours of receipt of an Anomaly Detection Thresholds File by the DCC; or

(b) for a Fast-Track Notification, within 24 hours of receipt of an Anomaly Detection Thresholds File by the DCC.

3.8 Where the DCC successfully validates and processes an Anomaly Detection Thresholds File submission from a User using a particular User ID then, the following provisions shall apply to the application of ADT and Warning Thresholds for that User and that User ID:

(a) in relation to each Service Request that would, were it to be targeted at a SMETS2+ Device, result in the sending of a Critical Command to that Device, but for which there is no entry with the Anomaly Detection Thresholds File, the ADT and Warning Threshold shall each be set to zero with a Time Period Applicable value of 1440;

(b) in relation to Service Reference Variant 6.23, if there is no entry that specifies a Time Period Applicable value of 1440, create an entry with a Time Period Applicable value of 1440 and with an ADT and Warning Threshold each set to zero;

(c) in relation to each other Service Request for which there is no entry within the Anomaly Detection Thresholds File, no value for the ADT or Warning Threshold shall be set; and

(d) in relation to each Service Request for which there is an entry in the Anomaly Detection Thresholds File the ADT, Warning Threshold and Time Period Applicable values shall be set to be equal to the values specified within the Anomaly Detection Thresholds File.

3.9 Where the ADT and Warning Thresholds have been successfully applied, the DCC shall update and close the relevant SMSR. Where any of the checks outlined at clause 3.5 fail, the DCC shall not amend the existing ADT and Warning Thresholds for that User and that User ID and shall update the SMSR to reflect this and notify the User of the reason for the failure.

3.10 Where the DCC has never successfully validated and processed an Anomaly Detection Thresholds File for a particular User in relation to a particular User ID then, for each Service Request that would, were it to be targeted at a SMETS2+ Device, result in the sending of a Critical Command to that Device, the DCC shall set each of the ADT and Warning Threshold to be zero with a Time Period Applicable value of 1440 for the relevant User and User ID.

4. Exceeding Anomaly Detection or Warning Thresholds

User and DCC Responsibilities: User Warning Threshold

4.1 Where the number of communications has exceeded the Warning Threshold, the DCC shall raise an Incident and send an email notification to the User's registered contact address on the DSMS.

4.2 Following any such notification, a User shall use the "View Service Management Incident" Functional Component within the SSI to obtain details on the Warning Threshold exceeded using the SMSR reference number provided within the email notification.

4.3 Each User shall investigate, and then update and assign the Incident to the DCC using the "Update Service Management Incident" Functional Component within the SSI.

User and DCC Responsibilities: User Set Anomaly Detection Threshold

4.4 Where the DCC has quarantined communications in accordance with the Service Request Processing Document the DCC shall raise an Incident and send an email notification to the affected User's registered contact address on the DSMS to inform the User of the ADT that has been exceeded.

4.4A In respect of each quarantined communication, the DCC shall also send a DCC Alert to the User who sent the communication to inform then that the communication has been quarantined.

4.5 The DCC shall make all such quarantined communications available to Users to whom they relate to download for a period of 120 hours from the point at which the communication was quarantined. At this point the DCC will immediately initiate the automated email notification process to notify the User that the communication has been quarantined. After this 120 hour time period has elapsed, the DCC shall archive all quarantined communications relating to the event for audit purposes and permanently delete them after 30 days. During the 30 day archive period, Users can access these archived communications only for the purposes of investigating a Major Security Incident.

4.6 Each User shall use the "View Service Management Incident" Functional Component within the SSI to obtain details on the ADT exceeded using the Incident reference number provided within the email notification. The User shall download a configurable report, as set out in clause 6.4 of this document, from the "reporting" Functional Component within the SSI, which shall include the list of quarantined communications in a CSV format.

4.7 Each User shall investigate and resolve the ADT exceeded event. Each User shall make a submission to the DCC (via its secure delivery method of choice, as from time to time specified on the SSI) indicating the action to be taken on each of the quarantined communications. The User shall include in such submission:

(a) the Incident reference number in the title of the submission; and

(b) a valid CSV file, updated with the required action for each communication ("Release" or "Delete"), Digitally Signed with a Private Key issued to the ARO for the purposes of CSV file signing, as set out in clause 6.5 of this document.

4.8 Each User shall update the Incident using the "Update Service Management Incident" Functional Component within the SSI and assign to the DCC for further action. The DCC shall:

(a) Check Cryptographic Protection applied to the CSV file, Confirm Validity of the Certificate used to Check Cryptographic Protection for the CSV file; and

(b) check that the format of the data is correct.

4.9 Upon successful validation of all of the above checks the DCC shall perform the actions on the quarantined communications, notify the User, update and close the Incident.

4.10 Where any of the above validation steps fail the DCC shall update the Incident, reassign it to the User and notify the User of the reason for the failure.

User and DCC Responsibilities: DCC Set Anomaly Detection Threshold

4.11 Pursuant to Section G6.6 of the Code the DCC shall set ADTs. Where a DCC set ADT has been exceeded, the DCC shall (subject to the provisions of clause 22.2 of the SMETS1 Supporting Requirements):

(a) quarantine the communication(s) that have exceeded the ADT;

(b) raise an Incident in accordance with the Incident Management Policy;

(c) determine the reasons for the Incident and take appropriate remedial action; and

(d) in respect of each quarantined communication, send a DCC Alert to the User who sent the communication to inform them that the communication has been quarantined.

4.12 DCC shall contact the User(s) impacted by the event by raising an Incident to notify them that their communication(s) have been quarantined. At an appropriate point during the investigation, DCC shall advise Users of the action that should be taken in respect of quarantined communications, which will be one of the following:

(a) that quarantined communications must be deleted;

(b) that the User may decide whether quarantined communications should be processed or deleted; or

(c) that no action should be taken by the User in respect of quarantined communications, which will result in the quarantined communications being archived for 30 days and subsequently deleted by the DCC.

4.13 Upon being advised of the action to be taken, the User shall raise a DCC Service Management Service Request (SMSR) via the SSI to obtain a reference number for use in its submission to DCC (which reference number will be generated by the SSI automatically). The User shall then send the DCC a Quarantined

Communications Action File which specifies actions in respect of each quarantined communication (which actions must, where relevant, correspond with the actions advised by the DCC). The submission of such file shall be made via the DCC's secure delivery method of choice (as from time to time specified on the SSI), and shall include:

(a) the DSMS Incident reference number notified in the title of the submission; and

(b) a valid CSV file, updated with the required action for each communication ("Release" or "Delete"), Digitally Signed with a Private Key issued to the ARO for the purposes of CSV file signing, as set out in clause 6.5 of this document.

4.14 The DCC shall make all such quarantined communications available to Users to whom they relate to download for a period of 120 hours from the point at which the communication was quarantined. At this point the DCC will immediately initiate the automated email notification process to notify the User that the communication has been quarantined. After this 120 hour time period has elapsed, the DCC shall archive all quarantined communications relating to the event and permanently delete them after 30 days. During the 30 day archive period, Users can access these archived communications only for the purposes of investigating a Major Security Incident.

4.15 The User shall download a configurable report, as set out in clause 6.4 of this document, from the "reporting" Functional Component within the SSI which shall include the quarantined communications(s) in a CSV format. Each User shall update the Incident using the "Update Service Management Incident" Functional Component within the SSI and assign the Incident to DCC for further action. The DCC shall:

(a) Check Cryptographic Protection applied to the CSV file, Confirm Validity of the Certificate used to Check Cryptographic Protection for the CSV file; and

(b) check that the format of the data is correct.

4.16 Within 24 hours of receipt of a Quarantined Communications Action File, the DCC shall validate that Quarantined Communications Action File and shall either:

(a) where the checks are successful, perform the actions on the quarantined communications and notify the User of successful completion of the notified actions once completed, via the SSI; or

(b) where the checks are unsuccessful, update and reassign the Incident and notify the User of the reason for the failure.

5. Exceptions Process

5.1 There are no exceptions to the process.

6. Communication Formats

6.1 All data sent to the DCC for use in the DCC Systems for the purposes of these Threshold Anomaly Detection Procedures shall be in the form of a Digitally Signed CSV file. The field separator shall be a comma "," and the record separator shall be a line feed character 0x0A. In the file descriptions set out in clause 6.3 to 6.5 of this document, the character "▲" indicates the record separator. Users may include, within such CSV files, consecutive comma separators to the left of a record separator to specify that a field has a null value. DCC shall interpret consecutive commas within a record to identify a null value.

6.2 Each User submitting a CSV file that is to be Digitally Signed using the Private Key associated with a File Signing Certificate shall, prior to Digitally Signing that file, ensure that:

(a) the CSV file is formatted to ensure that each record has a separator which is a 0x0A character and that any 0x0D character is removed from the file; and

(b) the last record in the CSV file is terminated with a 0x0A character.

Anomaly Detection Thresholds File

6.3 Each Anomaly Detection Thresholds File shall be generated in accordance with the procedure set out immediately below.

(a) (a) an "initial" CSV file shall be created, which shall contain the following records:

(i) UserID ▲

(ii) Sequence_Number ▲

(iii) Service_Reference_Variant, Warning_Threshold, Quarantine_Threshold, Time_Period_Applicable, (repeated for each applicable Service Reference Variant to be used) ▲

(b) a File Signing Certificate_ID shall be appended as a record to the end of the "initial" CSV file, comprising:

(i) all of the attributes contained within the 'Issuer' field in the File Signing Certificate, including attribute names, equals signs and values, which shall be encoded in URL format such that it does not contain any special characters, followed by a comma; and

(ii) the Certificate serial number obtained from the 'serialNumber' field in the File Signing Certificate, followed by a 0x0A character;

(c) a Digital Signature shall be generated from the "initial" CSV file and appended as a record to the end of the CSV file, in accordance with the procedure set out in clause 6 of this document; and

(d) where the fields are defined as follows:

(i) The UserID is the EUI-64 identifier obtained as part of the ID Allocation Procedure.

(ii) The Sequence_Number is a positive integer that is greater than zero and which is greater than the Sequence_number included within any prior Anomaly Detection Thresholds File containing the same UserID submitted by the relevant User.

(iii) The Service Reference Variant is the number set out in the DCC User Interface Specification (DUIS) for the Service Request.

(iv) The warning threshold field shall be populated with an integer value that is greater than or equal to zero.

(v) The quarantine threshold field shall be populated with an integer value that is greater than or equal to zero.

(vi) The Time Period Applicable is populated with a number that represents the measurement interval for the threshold in minutes, which shall be an integer value that is greater than or equal to one and less than or equal to 43200.

Quarantined Communications Report File

6.4 Each Quarantined Communications Report File shall contain the following fields:

(a) Event_Reference, Service_Reference_Variant, Critical_Indicator, Date/time, Originator_ID, Target_ID, Counter, (repeated for each quarantined communication uploaded by the User) ▲; and

(b) where the fields are defined as follows:

(i) The Event Reference is generated by the DCC for a particular instance of an ADT or Warning Threshold being exceeded.

(ii) The Service Reference Variant is the number set out in DUIS for the Service Request.

(iii) The Critical Indicator indicates whether the Service Request is Critical or Non-Critical, which shall be set to 'C' or 'NC'.

(iv) The Date/time field is the date and time when the communication was placed in quarantine, which will be of the format *DD/MM/YYYY hh:mm:ss*.

(v) Originator ID, Target ID and Counter fields are equivalent to the "RequestID", as set out in DUIS, for each quarantined communication.

Quarantined Communications Action File

6.5 Each Quarantined Communications Action File shall be generated in accordance with the procedure set out immediately below.

(a) an "initial" CSV file shall be created, which shall contain the following records:

(i) UserID ▲

(ii) Event_Reference, Service_Reference_Variant, Critical_Indicator, Date/time, Originator_ID, Target_ID, Counter, Action (repeated for each quarantined communication uploaded by the User) ▲

(b) a File Signing Certificate_ID shall be appended as a record to the end of the "initial" CSV file, comprising:

(i) all of the attributes contained within the 'Issuer' field in the File Signing Certificate, including attribute names, equals signs and values, which shall be encoded in URL format such that it does not contain any special characters, followed by a comma;

(ii) the Certificate serial number obtained from the 'serialNumber' field in the File Signing Certificate, followed by a 0x0A character; and

(c) a Digital Signature shall be generated from the "initial" CSV file and appended as a record to the end of the CSV file, in accordance with the procedure set out in clause 6 of this document; and

(d) where the fields are defined as follows:

(i) The UserID is the EUI-64 obtained as part of the ID Allocation Procedure.

(ii) The Event Reference is generated by the DCC for a particular instance of an ADT or Warning Threshold being exceeded.

(iii) The Service Reference Variant is the number set out in DUIS for the Service Request.

(iv) The Critical Indicator indicates whether the Service Request is Critical or Non-Critical, which shall be set to 'C' or 'NC'.

(v) The Date/time field is the date and time when the communication was placed in quarantine, which will be of the format DD/MM/YYYY hh:mm:ss.

(vi) Originator ID, Target ID and Counter fields are equivalent to the "RequestID", as set out in DUIS, for each quarantined communication.

(vii) The Action field shall be created and populated by the User for each quarantined communication with the required action, which shall have a value of "Delete" or "Release".

7. File Signing the "input" CSV File

7.1 An "input" CSV file will be finalised for communication by applying a Digital Signature to the end of the file.

7.2 The Private Key corresponding with the File Signing Certificate used for Digitally Signing the "input" CSV file shall be stored on a cryptographic token, supplied by the DCC in accordance with the SMKI RAPP.

7.3 Each User wishing to use the Private Key corresponding with a File Signing Certificate to apply a Digital Signature to an "input" CSV file and to append such Digital Signature record to the end of the "input" CSV file shall:

(a) Digitally Sign the content in the "input" CSV file, using a Private Key corresponding with the File Signing Certificate in accordance with the FIPS 186-4 Digital Signature Standard and using the parameters for signing as set out in clause 7.4; and

(b) convert the Digital Signature to Base64 format and append the Base64 encoded Digital Signature, as a record, to the end of the "input" file, followed by a 0x0A character, to create the "finalised" CSV file.

7.4 The parameters used for signing will be:

(a) Hashing algorithm: SHA-256, as specified in FIPS 180-4;

(b) Signing Method: The RSASSA – PKCS - v1.5 Digital Signature Algorithm specified in Section 5.5 of FIPS 186-4; and

(c) Key Length: 2048.

7.5 The DCC shall provide a software utility for the purposes of Digitally Signing files, which a User may choose to utilise in order to meet its obligations:

(a) to format such files so that the correct field separators and record separators are used;

(b) in respect of obligations to append a File Signing Certificate_ID to CSV files where required; and

(c) to Digitally Sign the “finalised” CSV file as set out in clause 7.3.

Version AB 9.0

APPENDIX AB

Service Request Processing Document

Contents

1 Introduction

1.1 This Appendix supplements Section H4 (Processing Service Requests) and sets out the obligations of the DCC and of each User in respect of communications via the DCC User Interface in respect of the following Services:

(a) Enrolment Services;

(b) Local Command Services;

(c) Core Communication Services; and

(d) Elective Communication Services.

2 Obligations of Users: Suspended Devices and Firmware

2.1 A User shall take all reasonable steps to ensure that it does not send Service Requests in relation to Devices that have an SMI Status of 'suspended', other than where:

(a) the Service Requests will (if Successfully Executed) result in the Device's Device Model becoming one that is listed on the Central Products List;

(b) it is necessary to do so in order to update the Device Security Credentials following a change of Responsible Supplier; or

(c) for SMETS1 Devices only, the User is requesting only the production of UTRNs for return to that User.

2.2 A User shall only send an 'Update Firmware' Service Request or an 'Update PPMID Firmware' Service Request in respect of a Device or a SMETS1 CH if:

(a) the User has received the following information:

(i) the OTA Header and the associated replacement Manufacturer Image;

(ii) a Digital Signature, created by the person who created the Manufacturer Image, across the concatenation of the OTA Header and the associated replacement Manufacturer Image; and

(iii) the Hash of the replacement Manufacturer Image;

(b) the User has successfully confirmed that the Digital Signature across the concatenation is that of the person who created the replacement Manufacturer Image (validated as necessary by reference to a trusted party);

(c) the User has generated its own Hash from the replacement Manufacturer Image, and confirmed that the Hash that the User has generated is the same as the Hash provided; and

(d) the User has confirmed that a Device Model associated with the replacement Manufacturer Image (as determined by the Hash and the information in the OTA Header) is currently on the Central Products List.

3 Obligations of Users: Pre-Commands and Signed Pre-Commands

3.1 Where a User receives a Pre-Command from the DCC, the User shall:

(a) Check Cryptographic Protection for the Pre-Command;

(b) Confirm Validity of the Certificate used to Check Cryptographic Protection for the Pre-Command; and

(c) subject to the requirements of Clause 3.1(a) and (b) being satisfied, Correlate the Pre-Command.

3.2 Where Correlation of the Pre-Command demonstrates that it is substantively identical to the Service Request that led to the Pre-Command, the User may:

(a) Digitally Sign the GBCS Payload of the Pre-Command to create the GBCS Payload of an associated Signed Pre-Command; and

(b) send the associated Signed Pre-Command with its appropriate wrapper and Digital Signature to the DCC.

3.3 Where applicable, Users must comply with their obligations under Section G3.25 (Supply Sensitive Check).

4 Obligations of the User: Communications Received in Error

4.1 Where a User receives a communication via the DCC User Interface which that User was not entitled to receive in accordance with this Code, the User shall notify the DCC in accordance with the Incident Management Policy.

5 Obligations of the DCC: SMETS2+ Communications Hub firmware

5.1 The DCC shall only send a communication to distribute different firmware to a SMETS2+ Communications Hub if:

(a) the DCC has received the replacement Manufacturer Image and a Digital Signature, created by the person who created the Manufacturer Image, across that Manufacturer Image;

(b) the DCC has received information about the Manufacturer Image sufficient to determine whether it is on the Central Products List;

(c) the DCC has successfully confirmed that the Digital Signature across the replacement Manufacturer Image is that of the person who created the replacement Manufacturer Image (validated as necessary by reference to a trusted party); and

(d) a Device Model associated with the replacement Manufacturer Image is currently on the Certified Product List, as determined by:

(i) the Hash the DCC calculates over the Manufacturer Image; and

(ii) the information about the Manufacturer Image provided pursuant to Clause 5.1(b).

5.2 The DCC shall notify relevant Users of its intention to activate replacement Manufacturer Images in relation to Communications Hubs at least 7 days in advance of doing so; provided that DCC need not notify Users in advance if the activation of the replacement Manufacturer Images is required for urgent security related reasons (and in such circumstances the DCC shall take reasonable steps to notify Users in advance of activating replacement Manufacturer Images or, where it has not notified them in advance, shall notify them of having done so as soon as is reasonably practicable after the event).

6 Obligations of the DCC: Processing Service Requests

6.1 Subject to Clause 18 (Obligations of the DCC: Non-Device Service Requests), where the DCC receives a Service Request from a User, the DCC shall send an Acknowledgement to the User, and (whether before or after such Acknowledgement is sent) apply the following checks:

(a) Verify the Service Request;

(b) confirm that the Service Request has been sent by a User whose right to send that Service Request has not been suspended in accordance with Section M8.5 (Suspension of Rights), and that such User is acting in a User Role which is an Eligible User Role for that Service Request;

(c) in the case of Non-Critical Service Requests (other than an 'Update Firmware' Service Request, an 'Update PPMID Firmware' Service Request, a 'CoS Update Security Credentials' Service Request or a 'Top Up Device' SMETS1 Service Request with a Command Variant value of 2) and SMETS1 Critical Service Requests, confirm that the SMI Status of the Device identified in the Service Request is: (i) 'commissioned'; (ii) 'installed not commissioned'; (iii) 'whitelisted'; or (iv) 'pending';

(d) Check Cryptographic Protection for the Service Request;

(e) Confirm Validity of the Certificate used to Check Cryptographic Protection for the Service Request, and confirm that the Certificate used to Check Cryptographic Protection for the Service Request has a Remote Party Role of “xmlSign”;

(f) subject to Clause 6.2, in the case of Non-Critical Service Requests and SMETS1 Critical Service Requests, confirm (using the Registration Data, the Device ID within the Service Request, and the relationship between the Device IDs and the MPRNs or MPANs in the Smart Metering Inventory) that the User sending the Service Request is a User that is or will be an Eligible User for that Service Request:

(i) for all times within any date range requested;

(ii) where there is no such date range, at the specified time for execution; or

(iii) where there is no date range and no date for execution is specified, at the time at which the check is being carried out;

(g) in the case of a 'CoS Update Security Credentials' Service Request:

(i) confirm that the User ID in the Certificate used to Check Cryptographic Protection of the Service Request is the same as the User ID in the Service Request;

(ii) confirm that the MPID that is used in the carrying out of the check referred to in Clause 6.1(f) above is the same as an MPID that is contained within the Subject X520 Organizational Unit Name field (as described in the Organisation Certificate Policy) of the Certificate used to Check Cryptographic Protection for the Service Request; and

(iii) confirm that the MPAN or MPRN (as relevant) associated with the target Device in the Smart Metering Inventory is the same as the MPAN or MPRN included within the ‘CoS Update Security Credentials' Service Request;

(iv) confirm that the number of Organisation Certificates contained within the Service Request is necessary and sufficient for the target Device;

(v) confirm that all of the replacement Organisation Certificates have a Remote Party Role of “supplier”;

(vi) confirm that the Key Usage of each such Organisation Certificate is compatible with the Trust Anchor Cell in relation to which the relevant Device Security Credentials are to be replaced;

(vii) where relevant, confirm that the SupplierPrepaymentTopUpFloorSeqNumber data item has been included within the Service Request;

(viii) confirm that the User ID contained within each of the Organisation Certificates included within the Service Request is associated with the User submitting the Service Request; and

(ix) confirm that the MPRN or MPAN included within the Service Request is Associated with the Device identified within the Service Request;

(h) in the case of a 'Restore HAN Device Log' or a 'Restore Gas Proxy Function Device Log' Service Request, confirm that the Device Log Data to be restored originates from a Communications Hub Function or Gas Proxy Function that forms (or formed immediately prior to its replacement) part of a Smart Metering System for which the User making such Service Request is (or, immediately prior to its replacement, was) the Responsible Supplier;

(i) in the case of an 'Update Firmware' Service Request or an 'Update PPMID Firmware' Service Request, confirm that the Hash calculated across the Manufacturer Image contained within the Service Request is the same as the entry within the Central Products List (as identified by the Device ID, information in the Smart Metering Inventory and the firmware version specified in the Service Request);

(j) in the case of any Service Request that contains any Certificates, Confirm Validity of those Certificates;

(k) in the case of any Service Request that is seeking to replace any part of the Device Security Credentials held on or in relation to a Device with information from an Organisation Certificate contained within that Service Request, confirm that:

(i) the Issuing OCA Certificate for each such Organisation Certificate is also contained within that Service Request; and

(ii) each Issuing OCA Certificate contained within that Service Request has been used to Issue at least one of the Organisation Certificates contained within that Service Request;

(l) in the case of an 'Update HAN Device Log' Service Request requesting the addition of a Smart Meter or a Standalone Auxiliary Proportional Controller to the Device Log of a Communications Hub Function confirm (using the Registration Data and the MPRN or MPAN in the Service Request) that the User sending the Service Request is a Responsible Supplier in respect of that MPRN or MPAN;

(m) in the case of a ‘Set CHF Sub GHz Configuration’ Service Request, that the settings requested would only allow a CHF to use Sub GHz Available Channels (as defined in the GBCS);

(n) in respect of a SMETS1 Critical Service Request, a 'Request Handover of DCC Controlled Device' SMETS1 Service Request, a ‘Top Up Device’ SMETS1 Service Request, or a 'CoS Update Security Credentials' Service Request relating to either a SMETS1 or SMETS2+ Device, confirm that the Service Request is not a Replay; and

(o) in the case of SMETS1 ‘Activate Firmware’ Service Requests, where the target Device is a SMETS1 CHF or a SMETS1 PPMID, confirm (using the Registration Data, the Device ID within the Service Request, and the relationship between the Device IDs and the MPANs in the Smart Metering Inventory) that the User sending the Service Request is the Import Supplier for the ESME on the same home area network.

6.2 The step set out at Clause 6.1(f) shall not apply in the following circumstances (and, where it is necessary to identify a Responsible Supplier, the DCC shall do so using the Registration Data, the Device ID within the Service Request, and the relationship between the Device IDs and the MPRNs or MPANs in the Smart Metering Inventory):

(a) an Import Supplier that is the Responsible Supplier for a Smart Metering System that shares a Communications Hub Function with a Smart Metering System that includes a Gas Smart Meter sends a 'Join Service' Service Request to join that Gas Smart Meter to a Gas Proxy Function;

(b) an Import Supplier that is the Responsible Supplier for a Smart Metering System that shares a Communications Hub Function with a Smart Metering System that includes a Gas Proxy Function sends a 'Restore GPF Device Log' Service Request to restore the Device Log of that Gas Proxy Function; or

(c) the Service Request has been sent by a User acting in the User Role of 'Other User'.

6.3 Where any of the checks in Clause 6.1 are not satisfied in respect of a Service Request, the DCC shall not be obliged to undertake any of the other checks that remain to be undertaken, and the DCC shall reject the Service Request (and, save where Clause 6.1(d) is not satisfied, notify the User of such rejection and of the reasons for such rejection via the DCC User Interface).

6.4 Clause 6.5 shall apply subject to:

(a) (in relation to SMETS2+ Service Requests only) Clauses 9 (Obligations of the DCC: 'Request Handover of DCC Controlled Device' Service Requests), and 11 (User and DCC Obligations: 'Join Service' and 'Unjoin' Service Requests for Pre-Payment Meter Interface Devices and Gas Smart Meters); and

(b) (for all Service Requests) Clauses 8 (Obligations of the DCC: 'CoS Update Security Credentials' Service Requests and (where relevant) Corresponding Pre-Commands), and 18 (Obligations of the DCC: Non-Device Service Requests).

6.5 Subject to Clause 6.4, where all of the requirements of Clause 6.1 are satisfied in respect of a Service Request, the DCC shall:

(a) where the Service Request is not a SMETS1 Service Request, Transform the Service Request and:

(i) in the case of a Non-Critical Service Request, send the associated Command in accordance with Clause 13 (DCC Obligations: Sending Commands); or

(ii) in the case of a Critical Service Request, send the Transformed Service Request to the User who submitted the Service Request;

(b) where the Service Request is a SMETS1 Service Request and the DCC is holding a stored SMETS1 Future Dated Critical Service Request which:

(i) is addressed to the same Device; and

(ii) has the same Service Reference Variant,

delete the stored SMETS1 Future Dated Critical Service Request;

(c) where the Service Request is a SMETS1 Service Request but is not a SMETS1 Future Dated Critical Service Request:

(i) identify the relevant SMETS1 Service Provider using the target Device ID within the Service Request;

(ii) create the contents of a Countersigned Service Request and Countersign it; and

(iii) send the Countersigned Service Request to the relevant SMETS1 Service Provider; and

(d) where the Service Request is a SMETS1 Future Dated Critical Service Request:

(i) create a stored SMETS1 Future Dated Critical Service Request (unless the execution date/time has been set by the User to Never); and

(ii) unless removed in the interim in accordance with Clause 6.5(b), at the execution date/time specified in the stored SMETS1 Future Dated Critical Service Request, re-apply all requirements of Clause 6.1 except for Clause 6.1(m) and, where all of the requirements of Clause 6.1 (other than 6.1(m)) are met:

(A) create the contents of a Countersigned Service Request and Countersign it;

(B) send the Countersigned Service Request to the relevant SMETS1 Service Provider; and

(C) once the DCC (including, where relevant, the SMETS1 Service Provider) has completed its processing in relation to the Countersigned Service Request, delete the stored SMETS1 Future Dated Critical Service Request.

7 Obligations of the DCC: Processing Signed Pre-Commands

7.1 Where the DCC receives a Signed Pre-Command from a User, the DCC shall provide an Acknowledgement to the User and (whether before or after such Acknowledgement is sent) apply the following checks:

(a) Verify the Signed Pre-Command;

(b) confirm that the Signed Pre-Command has been sent by a User whose right to send that message has not been suspended in accordance with Section M8.5 (Suspension of Rights), and that such User is acting in a User Role which is an Eligible User Role for a Service Request of the type corresponding with the Signed Pre-Command;

(c) Check Cryptographic Protection for the Signed Pre-Command;

(d) Confirm Validity of the Certificate used to Check Cryptographic Protection for the Signed Pre-Command;

(e) confirm that the Certificate used to Check Cryptographic Protection for the Signed Pre-Command has a Remote Party Role of “xmlSign”; and

(f) in the case of any Signed Pre-Command that is seeking to replace any part of the Device Security Credentials held on or in relation to a Device with information from an Organisation Certificate contained within that Signed Pre-Command, confirm that:

(i) the Issuing OCA Certificate for each such Organisation Certificate is also contained within that Signed Pre-Command; and

(ii) each Issuing OCA Certificate contained within that Signed Pre-Command has been used to Issue at least one of the Organisation Certificates contained within that Signed Pre-Command.

7.2 Subject to Clauses 14 (Obligations of the DCC: Orchestration of Service Requests), where all of the requirements of Clause 7.1 are satisfied, the DCC shall send the associated Command in accordance with Clause 13 (DCC Obligations: Sending Commands).

7.3 Where any of the checks in Clause 7.1 are not satisfied in respect of a Signed Pre- Command, the DCC shall not be obliged to undertake any of the other checks that remain to be undertaken, and the DCC shall:

(a) reject the Signed Pre-Command; and

(b) save where Clause 7.1(c) is not satisfied, notify the User of such rejection and of the reasons for such rejection via the DCC User Interface.

8 Obligations of the DCC: 'CoS Update Security Credentials' Service Requests and (where relevant) Corresponding Pre-Commands

8.1 The following shall apply in respect of each 'CoS Update Security Credentials' Service Request which is not a SMETS1 Service Request:

(a) where all of the requirements of Clause 6.1 are satisfied in respect of such a Service Request, the DCC shall send a Digitally Signed communication containing the 'CoS Update Security Credentials' Service Request (a Countersigned Cos Service Request) to the CoS Party; and

(b) following receipt of the Countersigned CoS Service Request, and immediately prior to creating any corresponding Update Security Credentials Signed Pre-Command referred to in Clause 8.2, the CoS Party shall:

(i) Check Cryptographic Protection for the Countersigned CoS Service Request received;

(ii) Confirm Validity of the Certificates used to Check Cryptographic Protection;

(iii) apply the checks set out in Clauses 6.1(a), 6.1(d), 6.1(e.), 6.1(f), 6.1(g), 6.1(j) and 6.1(k) to the Service Request included within the Countersigned CoS Service Request; and

(iv) confirm that the Service Request is not a Replay.

8.2 Where, in respect of the communication received in relation to a 'CoS Update Security Credentials' Service Request, the requirements of Clause 8.1(b) are satisfied, the CoS Party shall:

(a) apply CoS Party Threshold Anomaly Detection in accordance with the requirements of Clause 20 (CoS Party Threshold Anomaly Detection), which may result in a cessation of processing of the Service Request by the CoS Party, but otherwise either;

(i) where the target Device of the original ‘Cos Update Security Credentials Service Request is a SMETS2+ Device,

(A) generate the GBCS Payload of an 'Update Security Credentials' Signed Pre- Command that is substantively identical to the 'CoS Update Security Credentials' Service Request;

(B) Digitally Sign the GBCS Payload;

(C) incorporate the Digitally Signed GBCS Payload and the original Service Request into a single communication and Digitally Sign the communication with a CoS Party XML Signing Key to create a CoS Authorisation Response; and

(D) send the signed CoS Authorisation Response to the DCC, or

(ii) where the target Device of the original ‘Cos Update Security Credentials Service Request is a SMETS1 Device:

(A) Digitally Sign the communication with a CoS Party XML Signing Key to create a CoS Authorisation Response; and

(B) send the signed CoS Authorisation Response to the DCC.

8.3 Where, in respect of a communication received in relation to a 'CoS Update Security Credentials' Service Request, the requirements of Clause 8.1(a) are not satisfied:

(a) the CoS Party shall not undertake any further processing of the communication, and shall notify the DCC; and

(b) the DCC shall notify the User that sent the original Service Request that the Service Request cannot be processed (such notification to be sent via the DCC User Interface).

8.4 Where the DCC receives a CoS Authorisation Response from the CoS Party, the DCC shall apply the following checks:

(a) check Cryptographic Protection for the CoS Authorisation Response;

(b) Confirm Validity of the Certificates used to Check Cryptographic Protection for the CoS Authorisation Response;

(c) confirm that the Remote Party Role of the Certificate used to Check Cryptographic Protection for the CoS Authorisation Response is ‘coSPartyXmlSign’;

(d) confirm that the CoS Authorisation Response is valid and well formed;

(e) confirm that the CoS Authorisation Response maps to a Countersigned CoS Service Request that was previously sent to the CoS Party;

(f) apply the checks set out in Clauses 6.1(a), 6.1(d), 6.1(e.), 6.1(f), 6.1(g), 6.1(j) and 6.1(k) to the Service Request contained within the CoS Authorisation Response;

(g) (in the circumstances where the target Device of the original ‘CoS Update Security Credentials Service Request is a SMETS2+ Device only) confirm that the Signed Pre-Command contained within the CoS Authorisation Response is substantively identical to the Service Request contained within the CoS Authorisation Response; and

(h) confirm that neither the CoS Authorisation Response, nor the Service Request contained within it is a Replay.

8.5 Subject to Clause 14 (Orchestration of Service Requests), where all of the requirements of Clause 8.4 are satisfied in respect of a CoS Authorisation Response received from the CoS Party, the DCC shall:

(a) (in the circumstances where the target Device of the original ‘CoS Update Security Credentials Service Request is a SMETS2+ Device) send a Command associated with the Signed Pre-Command contained within the CoS Authorisation Response in accordance with Clause 13 (DCC Obligations: Sending Commands); or

(b) (in the circumstances where the target Device of the original ‘CoS Update Security Credentials Service Request is a SMETS1 Device) Countersign the CoS Update Security Credentials Service Request and send the Countersigned Service Request to the relevant SMETS1 Service Provider in accordance with the requirements of Clause 14.

8.6 Where any of the checks in Clause 8.4 are not satisfied in respect of a CoS Authorisation Response received from the CoS Party, the DCC shall:

(a) not be obliged to undertake any of the other checks that remain to be undertaken, and the DCC shall reject the CoS Authorisation Response;

(b) save where Clause 8.4(c) is not satisfied, notify the CoS Party of such rejection and of the reasons for such rejection; and

(c) notify the User that sent the original 'CoS Update Security Credentials' Service Request.

9 Obligations of the DCC: 'Request Handover of DCC Controlled Device' Service Requests

9.1 This Clause 9 only applies to 'Request Handover of DCC Controlled Device' Service Requests that are not SMETS1 Service Requests. Where all of the requirements of Clause 6.1 are satisfied in relation to such a Service Request, the DCC shall:

(a) generate the corresponding GBCS Payload (corresponding in this case meaning that the Service Request and the GBCS Payload request the replacement of the same Device Security Credentials on the same Device at the same time);

(b) Digitally Sign the GBCS Payload; and

(c) Confirm Validity of any Certificates contained within the communication.

9.2 Where all of the requirements of Clause 9.1 are satisfied in respect of such a communication, the DCC shall send the associated Command in accordance with Clause 13 (DCC Obligations: Sending Commands).

9.3 Where any of the checks in Clause 9.1 are not satisfied in respect of such a communication, the DCC shall not undertake any of the other checks that remain to be undertaken, and the DCC shall reject the communication and notify the User that sent the original 'Request Handover of DCC Controlled Device' Service Request (such notification to be sent via the DCC User Interface).

10 User and DCC Obligations: 'Restore HAN Device Log' Service Requests

10.1 Where a Supplier Party replaces a Communications Hub (other than a SMETS1 CH) in a premises then that Supplier Party must, as soon as reasonable practicable after the replacement, send the necessary Service Requests to the DCC to ensure that:

(a) the Device Log of the new Communications Hub Function replicates that of the old Communications Hub Function;

(b) the Device Log of the new Gas Proxy Function is replaced with that of the old Gas Proxy Function (or replicates that of the old Gas Proxy Function);

(c) following steps (a) and (b) above, the new Gas Proxy Function is added to the Device Log of the Gas Smart Meter; and

(d) following the step set out in (c) above, the Communications Hub Function and the Gas Proxy Function comprising the Communications Hub that has been replaced are decommissioned (through the sending of a 'Decommission Device' Service Request).

10.2 An Import Supplier shall not send a Service Request to add or remove a Gas Proxy Function to or from the Device Log of a Gas Smart Meter other than as part of managing the replacement of a Communications Hub (by it or another Responsible Supplier) pursuant to Clause 10.1.

10.3 The DCC shall, following the decommissioning of a Communications Hub Function and the associated Gas Proxy Function (arising as a consequence of the processing of a 'Decommission Device' Service Request), send a DCC Alert to all Responsible Suppliers and Network Parties for Smart Metering Systems which incorporated either or both of those Devices, notifying them of the decommissioning (other than to the Responsible Supplier which sent the 'Decommission Device' Service Request).

10.4 The DCC shall, where it has processed a Service Request which successfully replaces the Device Log of a Communications Hub Function, send a DCC Alert to all Responsible Suppliers for that Communications Hub Function (other than the Responsible Supplier which sent the original Service Request) notifying them of the replacement.

10.5 The DCC shall, where it has processed a Service Request to successfully replace the Device Log of a Gas Proxy Function, send a DCC Alert to the Gas Supplier who is the Responsible Supplier for that Gas Proxy Function (save where it is the Gas Supplier that has sent the Service Request).

11 Obligations of the DCC: 'Join Service' and 'Unjoin' Service Requests for Pre- Payment Meter Interface Devices and Gas Smart Meters

11.1 Where all of the requirements of Clause 6.1 are satisfied in respect of a 'Join Service' or 'Unjoin Service' Service Request for a Pre-Payment Meter Interface Device, or a Gas Smart Meter and where the Service Request is not a SMETS1 Service Request, the DCC shall:

(a) Transform the Service Request;

(b) where a Pre-Payment Meter Interface Device is to be joined to a Gas Smart Meter, include within the resultant communication the Device Certificate of the relevant Gas Smart Meter that has a key usage of 'keyAgreement';

(c) where a Gas Smart Meter is to be joined to a Pre-Payment Meter Interface Device, include within the resultant communication the Device Certificate of the relevant Pre-Payment Meter Interface Device that has a key usage of 'keyAgreement';

(d) where the resultant communication is destined for a Pre-Payment Meter Interface Device, Digitally Sign the Communication and send the associated Command in accordance with Clause 13 (Obligations of the DCC: Sending Commands); and

(e) where the resultant communication is ultimately destined for a Gas Smart Meter, send the resultant communication as a Pre-Command to the User that sent the original Service Request.

11.2 Where the DCC receives a Response in respect of a Command sent to join or unjoin a Pre-Payment Meter Interface Device, the DCC shall send the Response (as a Service Response) to the User that sent the corresponding Service Request.

12 Threshold Anomaly Detection

12.1 The DCC shall apply Threshold Anomaly Detection where an Anomaly Detection Threshold has been established under Section G6 (Anomaly Detection Thresholds) in respect of the SMETS1 Service Request, Transformed Service Request or Signed Pre- Command.

12.2 Where the DCC applies Threshold Anomaly Detection to either a SMETS1 Service Request, a Transformed Service Request or a Signed Pre-Command and the check is failed, the DCC shall, subject to Clause 22 (Anomaly Detection) of the SMETS1 Supporting Requirements, notify the User and quarantine the SMETS1 Service Request, Transformed Service Request or Signed Pre-Command.

12.3 Where the DCC has quarantined a SMETS1 Service Request, Transformed Service Request or Signed Pre-Command it shall maintain such quarantine until:

(a) such time as the relevant User instructs the DCC to process the Service Request or Signed Pre-Command, in which case the DCC shall continue to process the Service Request or Signed Pre-Command in accordance with the provisions of this Service Request Processing document;

(b) the Service Request or Signed Pre-Command is confirmed by the User to be anomalous or to otherwise require deletion, in which case the DCC shall delete it from the DCC Systems; or

(c) the Service Request or Signed Pre-Command is required to be deleted in accordance with the Threshold Anomaly Detection Procedures, in which case the DCC shall delete it from the DCC Systems.

12.4 Where the DCC applies Threshold Anomaly Detection (other than in relation to a value of the type referred to in (b)(ii) of the definition of Anomaly Detection Threshold) to a Signed Pre-Command, Transformed Service Request or SMETS1 Service Request (for the purposes of this Clause, each being a "**Relevant Communication**"), the DCC shall:

(a) determine the Service Reference Variant of the Service Request that pertains to the Relevant Communication;

(b) determine the cumulative number of all other Relevant Communications to which that Service Reference Variant pertains that it has processed over the period of time to which the Anomaly Detection Threshold relates;

(c) increment the cumulative number by 1; and

(d) compare that incremented cumulative number to the relevant Anomaly Detection Threshold.

13 DCC Obligations: Sending Commands

13.1 Where the DCC is required to send a Command (other than an Instruction), it shall only apply any necessary Message Authentication Code to the relevant communication and send the resulting Command if:

(a) Threshold Anomaly Detection has been applied to the associated Transformed Service Request or Signed Pre-Command (or, where in response to a Service Request from an Eligible User a Command is to be Digitally Signed by the DCC, that Command prior to the addition of a Message Authentication Code); and

(b) either (i) the Threshold Anomaly Detection check is passed; or (ii) the User that sent the original Service Request or Signed Pre-Command has instructed DCC to process a quarantined Service Request or Signed Pre-Command in accordance with Clause 12.3(a).

13.2 Where the requirements of Clause 13.1 are met, the DCC shall apply the required Message Authentication Code (as required by the GB Companion Specification) to the relevant communication to create a Command and send that Command to (as specified in the originating Service Request):

(a) the relevant Device (provided that this option is only available in respect of Devices associated with Commissioned Communications Hub Functions); and/or

(b) the User who sent the originating Service Request via the DCC User Interface.

14 DCC Obligations: Sending Countersigned Service Requests

14.1 Where the DCC is required to send a Countersigned Service Request, it shall only Countersign the relevant communication and send the resulting Countersigned Service Request to the relevant SMETS1 Service Provider if:

(a) Threshold Anomaly Detection has been applied to the Service Request (provided that the DCC shall not be required to apply Threshold Anomaly Detection in relation to Anomaly Detection Thresholds of the type referred to in Sub-Paragraph (b)(ii) of the definition of Anomaly Detection Threshold; and

(b) either (i) the Threshold Anomaly Detection check is passed; or (ii) the User that sent the original Service Request has instructed DCC to process the quarantined Service Request in accordance with Clause 12.3(a).

15 Orchestration of Service Requests

15.1 In the case of a Service Request for a Sequenced Service, the DCC shall:

(a) where the Service Request is not a SMETS1 Service Request, only send the Command following the Successful Execution of the Command resulting from the Service Request upon which such Sequenced Service is dependent; and

(b) where the Service Request is a SMETS1 Service Request, only send the Countersigned Service Request to the relevant SMETS1 Service Provider following the Successful Execution of the Equivalent Step(s) resulting from the Service Request upon which such Sequenced Service is dependent.

15.2 The DCC shall ensure that it sends each 'Update Security Credentials' Command resulting from a 'CoS Update Security Credentials' Service Request as close to the specified execution time as is reasonably practicable whilst still allowing time for the Command to be received and executed by the relevant Device.

15.3 The DCC shall not continue to process any Service Requests (or associated Pre- Commands or Signed Pre-Commands) where the services have been cancelled in accordance with Sections H3.18 to H3.20 (Cancellation of Future-Dated or Scheduled Services).

16 Obligations of a SMETS1 Service Provider: Countersigned Service Request Processing

16.1 Where a SMETS1 Service Provider receives a Countersigned Service Request from the DCC, the SMETS1 Service Provider shall apply the following checks:

(a) Check Cryptographic Protection for both the Countersigned Service Request and, if it does not contain a message derived from an 'Update Firmware' Service Request, for the Service Request included within it;

(b) Confirm Validity of all Certificates used to Check Cryptographic Protection for both the Countersigned Service Request and, if it does not contain a message derived from an 'Update Firmware' Service Request, for the Service Request included within it;

(c) confirm it is the relevant SMETS1 Service Provider for the Device(s) identified in the Countersigned Service Request;

(d) if the Countersigned Service Request contains a Critical Service Request, a 'CoS Update Security Credentials' SMETS1 Service Request or a 'Request Handover of DCC Controlled Device' SMETS1 Service Request, apply the checks at Clause 6.1, except for those at Clauses 6.1 (d) and (e), to the Service Request contained within the Countersigned Service Request; and

(e) if the Countersigned Service Request contains a message derived from an 'Update Firmware' Service Request, then:

(i) if it is destined for a Communications Hub Function or a PPMID, Check Cryptographic Protection for the Upgrade Image contained within Countersigned the Service Request using the relevant Device Security Credentials that relate to the Import Supplier for the ESME which is on the same home area network as the relevant SMETS1 CHF or PPMID (as the context requires) and Confirm Validity for all of the Certificates used to Check Cryptographic Protection; or

(ii) if it is destined for a Smart Meter, Check Cryptographic Protection for the Upgrade Image contained within the Countersigned Service Request using the relevant Device Security Credentials held that relate to the Responsible Supplier for the Device and Confirm Validity for all of the Certificates used to Check Cryptographic Protection.

16.2 Only where all of the requirements of Clause 16.1 are satisfied, the SMETS1 Service Provider shall:

(a) in the case of a Countersigned Service Request that contains a Service Request with Service Reference Variant 2.2 (Top Up Device):

(i) apply Threshold Anomaly Detection in the circumstances where a relevant Anomaly Detection Threshold of the type referred to in Sub-Paragraph (b)(ii) of the definition of Anomaly Detection Threshold has been set; and

(ii) if the checks in Sub-Clause (a)(i) are passed, undertake further processing as required by the SMETS1 Supporting Requirements;

(b) in relation to any other Service Request, and any message derived from an 'Update Firmware' Service Request, contained within a Countersigned Service Request, for the target Device identified within the Service Request:

(i) apply Threshold Anomaly Detection in the circumstances where a relevant Anomaly Detection Threshold has been set pursuant to Section G6.6(b); and

(ii) if the checks in Sub-Clause (b)(i) are passed, ensure that the Equivalent Steps are taken and that either the resultant SMETS1 Response or a SMETS1 Service Provider Alert is generated; and

(c) ensure that any resulting SMETS1 Response or SMETS1 Alert is Digitally Signed, and send any such SMETS1 Response or SMETS1 Alert to the DCC.

17 Obligations of the DCC: Service Responses and Alerts

17.1 Where the DCC receives an Alert from a Communications Hub Function, the DCC shall Digitally Sign the Alert, and send it as a DCC Alert to (as specified in the DCC User Interface Specification) the Responsible Supplier(s), the Electricity Distributor and/or the Gas Transporter for the Smart Metering Systems of which the Communications Hub Function forms part (as identified in the Registration Data).

17.2 Where the DCC receives from a Device either a Response that is destined for a Remote Party or an Alert which is destined for one or more Remote Parties and/or Supplementary Remote Parties, then the DCC shall send the Response (as a Service Response) or the Alert (as a DCC Alert or Device Alert) to those Remote Parties and/or Supplementary Remote Parties as prescribed by the DCC User Interface Specification.

17.3 Where the DCC receives from an SMETS1 Service Provider:

(a) a SMETS1Response;

(b) a SMETS1 Alert; or

(c) a S1SP Alert,

which is destined for one or more Remote Parties and/or Supplementary Remote Parties, then the DCC shall Countersign the relevant communication and send it to those Remote Parties and/or Supplementary Remote Parties as prescribed by the DCC User Interface Specification as a Countersigned SMETS1 Response, a Countersigned SMETS1 Alert or Countersigned SISP Alert.

17.4 Where the DCC successfully processes a Service Request to replace the Security Credentials of a User that are held on a Device, or to place a User's Security Credentials on to a Device, then (other than to the extent that the User is notified via a Service Response) the DCC shall send a DCC Alert to the relevant User informing it of the change.

17.5 Where the DCC successfully processes a Service Request that changes the Security Credentials of a User that are held by a SMETS1 Service Provider in relation to a Device then (other than to the extent that the User is notified via a Countersigned SMETS1 Response) the DCC shall send a DCC Alert to the relevant User informing it of the change.

17.6 Where the DCC receives a Response or an Alert from a Device which is destined for an Unknown Remote Party, the DCC shall:

(a) Check Cryptographic Protection for the Response or Alert;

(b) Confirm Validity of the Certificate used to Check Cryptographic Protection for the Response or Alert; and

(c) subject to (a) and (b) being successful, send the Response (as a Service Response) or the Alert (as a Device Alert or DCC Alert) to the recipient(s) identified in the Response or Alert.

17.7 Where the DCC receives a Sub GHz Alert (as defined in the GBCS) from a Communications Hub Function, the DCC shall:

(a) Check Cryptographic Protection for the Sub GHz Alert;

(b) Confirm Validity of the Certificate used to Check Cryptographic Protection for the Sub GHz Alert; and

(c) subject to (a) and (b) being successful, create a DCC Alert containing the Sub GHz Alert, Digitally Sign the DCC Alert, and send the signed DCC Alert to the Responsible Supplier(s) for the Smart Metering System(s) of which the Communications Hub Function forms part (as identified using the Registration Data).

17.8 Where the DCC receives an Alert, the Alert shall be subject to the following Alert Management Mechanism:

(a) When the number of Alerts from a given Device within a defined rolling time window [T] exceeds the defined red threshold value [A] the system will begin to count the number of Alerts from that Device on a per Alert Code basis.

(b) If any individual Alert Code count within a defined rolling time window [R] exceeds the defined configured threshold value [B] then that originating Device/Alert Code combination will be labelled with 'HighAlertRate'.

(c) If an Alert Code is marked as 'HighAlertRate' for a Device, then only one in a defined number of such Alerts [N] will be processed. All other Alerts with that same Alert Code from the same Device will be consolidated.

(d) If within a period of the Alert storm protection maximum time limit [P] the Alert Code fails to reach [N], an Alert will be sent to the User. All other Alerts with that same Alert Code from the same Device will be consolidated.

(e) Once the rate of Alerts for the Device/Alert Code combination falls below the defined threshold [B] in the defined rolling period [R] then the Alert consolidation will stop and the recipient(s) identified in the Response or Alert informed.

17.9 Where the DCC receives an Alert subject to the process described in Section 17.8, the Alert will be subject to the following configuration parameters:

(a) When the number of Alerts from a given Device within the defined rolling time window [T] exceeds a defined amber threshold [M], an incident will be raised to notify the User.

(b) If a Device/Alert Code combination has been labelled 'HighAlertRate' and an incident has been raised to notify the User, a new incident will not be created until the rolling deadband time period [D] has elapsed.

(c) Where [M] or [A] have been exceeded within the defined rolling time period [R], the DCC will only create incidents when the amber threshold incident creation [MIC], red threshold incident creation [AIC] and Alert storm protection incident creation [PIC] parameters have been set to 'on'. When these values are set to 'off', no incident or accompanying notification will be created.

17.10 The defined parameters used in the Alert Management Mechanism detailed in Section 17.8, the configuration parameters detailed in Section 17.9 and the Alerts that are to be exempt from this mechanism are specified in the Traffic Management Mechanism Document. Any changes to this document shall be prepared and consulted upon by the DCC and approved by the Panel.

18 Obligations of the DCC: Non-Device Service Requests

18.1 Where the DCC receives a Non-Device Service Request from a User, the obligations of the DCC under this Appendix shall be modified as follows (and where a Non-Device Service Request is not specifically identified below, they shall be applied un-modified):

(a) the DCC shall not send an Acknowledgement in respect of the Service Request;

(b) the checks set out in Clause 6.1 shall be modified as follows:

(i) the check set out in Clause 6.1(c) does not apply to the following Service Requests:

(A) 'Update Inventory';

(B) 'Read Inventory';

(C) 'Request WAN Matrix';

(D) 'Device Pre-notification';

(E) 'Communications Hub Status Update- Install Success';

(F) 'Communications Hub Status Update - Install No SM WAN';

(G) 'Communications Hub Status Update – Fault Return'; and

(H) 'Communications Hub Status Update – No Fault Return'; and

(ii) the check set out in the Clause 6.1(f) does not apply to the following Service Requests:

(A) 'Read Inventory';

(B) 'Request WAN Matrix';

(C) 'Device Pre-notification';

(D) 'Communications Hub Status Update- Install Success';

(E) 'Communications Hub Status Update - Install No SM WAN';

(F) 'Communications Hub Status Update – Fault Return'; and

(G) 'Communications Hub Status Update – No Fault Return';

(c) the DCC shall not, in any event, be required to apply Threshold Anomaly Detection in relation to Non-Device Service Requests;

(d) where the checks set out in Clause 6.1 (as modified by this Clause 18) are satisfied, the DCC shall not Transform the Service Request or Countersign a Countersigned Service Request (as would otherwise be required by Clause 6) and shall instead send the User a Service Response notifying the User whether or not the Non-Device Service Request has been successful, and where successful:

(i) in the case of any Non-Device Service Request that changes or creates information held (or intended to be reflected) on the DCC Systems (including the Smart Metering Inventory), update the information held on DCC Systems accordingly; and/or

(ii) in the case of a 'Read Inventory' or 'Request WAN Matrix' Service Request, include within the Service Response the relevant information requested by the Service Request;

(iii) in the case of a 'Device Pre-Notification' Service Request, add the relevant Device to the Smart Metering Inventory with an SMI Status of 'pending';

(iv) in the case of a 'Create Schedule' Service Request,

(A) create a schedule of the Service Request type identified in the 'Create Schedule' Service Request;

(B) include within the Service Response the identifier of any schedule that has been successfully created;

(C) at each point in time set out in the schedule (and subject to the further arrangements set out in the DCC User Interface Specification), create a Service Request (without a Digital Signature from the User) of the appropriate type and in relation to the relevant Device (in each case as specified in the original 'Create Schedule' Service Request);

(D) process the Service Requests referred to in (C) above in accordance with Clause 6 as if they had been received from the User that sent the original 'Create Schedule' Service Request, provided that the checks identified under Clause 6.1(c) and 6.1(d) do not apply;

(v) in the case of a 'Read Schedule' Service Request, where it is received from the same User that sent the originating 'Create Schedule' Service Request for all schedules identified within it, include within the Service Response details of the relevant schedule(s) so identified (and otherwise reject the 'Read Schedule' Service Request, and notify (via the Service Response) the User that sent the Service Request of such rejection);

(vi) in the case of a 'Delete Schedule' Service Request, where it is received from the same User that sent the originating 'Create Schedule' Service Request for all schedules identified within it, delete the relevant schedule(s) so identified (and otherwise reject the 'Delete Schedule' Service Request, and notify (via the Service Response) the User that sent the Service Request of such rejection);

(vii) in the case of a 'Decommission Device' Service Request:

(A) set the SMI Status of the relevant Device to 'decommissioned';

(B) where the relevant Device is a Smart Meter or a Standalone Auxiliary Proportional Controller, disassociate the Device in the Smart Metering Inventory from any MPRN or MPAN with which it is associated; and

(C) where the relevant Device is a Communications Hub Function, set the SMI status of the associated Gas Proxy Function to 'decommissioned'; or

(viii) in the case of an 'Update Firmware' Service Request:

(A) include within the Service Response the details of any Devices that were listed within the Service Request to which, by virtue of the checks DCC has carried out, DCC does not propose to send a communication to update the firmware; and

(B) to all other Devices so listed, send a communication to update the firmware of those Devices ensuring that the communication reaches the SMETS1 CHF (in the case of updates to a SMETS1 CHF) or (in the case of updates to all other Devices) the Communications Hub Functions associated with all such Devices (in each case, within the timescales specified in the DCC User Interface Services Schedule). Where the Service Request relates to SMETS1 Devices, the DCC shall Digitally Sign the resulting communication that it sends to the SMETS1 Service Provider; or

(ix) in the case of an 'Update PPMID Firmware' Service Request:

(A) include within the Service Response the details of any Devices that were listed within the Service Request to which, by virtue of the checks DCC has carried out, DCC does not propose to send a communication to update the firmware; and

(B) to all other Devices so listed, send a communication to update the firmware of those Devices ensuring that the communication reaches the Communications Hub Functions associated with all such Devices (in each case, within the timescales specified in the DCC User Interface Services Schedule).

19 Incident Management

19.1 Where the Device Security Credentials of a Device erroneously include Data from one or more of a Party's Organisation Certificates, that Party shall cooperate with other Parties in order to rectify the position (including, were necessary, by sending Service Requests to update the Device Security Credentials).

20 CoS Party Threshold Anomaly Detection

20.1 For each User ID that each Supplier Party uses in relation to submitting CoS Update Security Credentials Service Requests, the CoS Party shall apply Threshold Anomaly Detection in accordance with the requirements of the Anomaly Detection Procedures (provided that the provisions relating to quarantining of Service Requests shall not apply) and Clauses 20.2 to 20.5.

20.2 For each such User ID, the Anomaly Detection Threshold used by the CoS Party shall be that most recently set by the relevant User in accordance with the Threshold Anomaly Detection Procedures and which applies to a 24 hour period for each calendar day for CoS Update Security Credentials Service Requests.

20.3 A ‘CoS Update Security Credentials’ Service Request shall be considered to ‘apply’ to a particular day if:

(a) The Service Request has been submitted as a Future Dated Service Request and the relevant execution time falls on that day; or

(b) The Service Request has been submitted as an On-Demand Service Request and the relevant Service Request has been received by the CoS Party on that day.

20.4 The CoS Party shall cease the processing of any ‘CoS Update Security Service Requests’ applying to a particular day, and submitted by a Supplier Party Using a particular User ID if the number of such Service

Requests applying in relation to that day exceeds the Anomaly Detection Threshold for that User ID (and a DCC Alert shall be sent to the User in such circumstances).

20.5 For the avoidance of doubt, Threshold Anomaly Detection applied by the CoS Party shall be applied across the sum of both SMETS1 and SMETS2+ Service Requests applying to a particular day.

21 Definitions and Interpretation

21.1 For the purposes of this Servicing Request Processing Document, the term:

(a) "CoS Authorisation Response" means a communication that, where it relates to a SMETS2+ Device, contains a 'CoS Update Security Credentials Service Request and an associated 'Update Security Credentials' Signed Pre-Command that has been Digitally Signed by the CoS Party or, where it relates to a SMETS1 Device, contains a 'CoS Update Security Credentials Service Request and has been Digitally Signed by the CoS Party.

(b) "CoS Party XML Signing Key", means a Private Key that has an associated Public Key that is contained within an Organisation Certificate that has a Remote Party Role of 'coSPartyXmlSign';

(c) "Countersigned CoS Service Request" has the meaning given to that term in Clause 8.1(a);

(d) "MPID" means one of the unique identifiers by which the eligible subscriber may be identified in the Party Details;

(e) "Key Usage" has the meaning ascribed to that term in the Organisation Certificate Policy;

(f) "SupplierPrepaymentTopUpFloorSeqNumber" has the meaning ascribed to that term in the DCC User Interface Specification; and

(g) Trust Anchor Cell has the meaning ascribed to that term in the GB Companion Specification.

Version AC 7.0

APPENDIX AC

Inventory Enrolment and Decommissioning Procedures

Contents

1. Overview

1.1 This Appendix supplements Sections H5 (Smart Metering Inventory and Enrolment Services) and H6 (Decommissioning and Suspension of Devices).

2. Smart Metering Inventory

2.1 The DCC shall establish and maintain the Smart Metering Inventory.

2.2 The DCC shall ensure that the Smart Metering Inventory reflects the most up-to-date information provided (or made available) to it from time to time in accordance with this Code (subject to Section F2.9 (Publication and Use by the DCC)).

2.3 Parties shall not seek to add Devices to the Smart Metering Inventory (and the DCC shall not add Devices to the Smart Metering Inventory) otherwise than in compliance with this Appendix.

2.4 Prior to delivering a Communication Hub to a Party pursuant to the Communications Hub Service, the DCC shall add the Communications Hub Function and Gas Proxy Function that comprise that Communications Hub to the Smart Metering Inventory (to be identified with an SMI Status of 'pending'); provided that such Devices may only be added to the Smart Metering Inventory where the Communications Hub is of a Device Model identified in the Central Products List.

2.5 No Party shall add Communications Hub Functions to the Smart Metering Inventory without also adding the Gas Proxy Function that forms part of the same Communications Hub (and vice versa).

2.6 Any User may send a Service Request requesting that the DCC adds a Device to the Smart Metering Inventory (to be identified with an SMI Status of 'pending'); provided that only Devices of (or forming part of) a Device Model that is identified in the Central Products List are eligible to be added to the Smart Metering Inventory. This Clause 2.6 does not apply to Type 2 Devices (which are covered in Clause 2.9).

2.7 The DCC shall not send any communication to a Device unless the Device is listed in the Smart Metering Inventory; save for communications sent for the purposes of testing under Section H14 (Testing Services).

2.8 In the case of Communications Hub Functions and Gas Proxy Functions, the only Communications Hubs that may be added to the Smart Metering Inventory (subject to Clause 12.3) are those that comprise either a SMETS1 CH or a Communications Hub that is to be provided by the DCC pursuant to the Communications Hub Service.

2.9 Any User may send a Service Request requesting that the DCC adds a Type 2 Device to the Smart Metering Inventory. For the avoidance of doubt, a Type 2 Device shall not be identified in the Central Products List, and shall have no SMI Status.

2.10 The Responsible Supplier for each Smart Metering System shall keep under review the information recorded in the Smart Metering Inventory in respect of the Devices that comprise that Smart Metering System. Where circumstances change or the Responsible Supplier identifies an error in such information, the Responsible Supplier shall submit Service Requests requesting that the DCC updates the Smart Metering Inventory (or, where it is not possible to do so, shall raise an Incident in accordance with the Incident Management Policy). Where a correction is made in respect of the relationship between one or more Smart Meters / Standalone Auxiliary Proportional Controllers and an MPAN and/or MPRN, then the DCC shall notify the Electricity Distributor and/or Gas Transporter for the affected MPANs and/or MPRNs.

2.11 Where a User other than the Responsible Supplier for a Smart Metering System becomes aware of an error in the information recorded within the Smart Metering Inventory in respect of a Device that comprises that Smart Metering System, it shall raise an Incident in accordance with the Incident Management Policy.

2.12 Where a User receives a Response or Alert other than via the SM WAN, the User shall, where the Response or Alert is listed in the DCC User Interface Specification as one that is required to be returned to the DCC, send a 'Return Local Command Response' Service Request containing the Response or Alert to the DCC.

3. Pre-Commissioning Obligations

Pre-Commissioning obligations in relation to SMETS2+ Devices

3.1 Where the relevant Device is a SMETS2+ Device, before:

(a) a Responsible Supplier sends a Service Request which may result in the sending of a Command to a Smart Meter, Standalone Auxiliary Proportional Controller, Gas Proxy Function or Type 1 Device; or

(b) the DCC delivers a Communications Hub (comprising a Communications Hub Function and a Gas Proxy Function) to a Party in accordance with the Communications Hub Service,

the Responsible Supplier or DCC (as the case may be) shall ensure that each Trust Anchor Cell on that Device which is required by the GB Companion Specification to be populated with credentials is populated with credentials in accordance with the requirements of Clause 3.2.

3.2 The requirements of this Clause 3.2 are that:

(a) each Trust Anchor Cell with the Remote Party Role listed in the table immediately below shall be populated with the Security Credentials from the Certificate (or, as indicated, one of the Certificates) identified in relation to that Remote Party Role in the second column of that table; and

(b) in each case the relevant Certificate shall have a keyUsage value which is the same as that of the Trust Anchor Cell it populates.

Remote Party Role	Certificate
Root	a Root OCA Certificate
Recovery	a DCC Recovery Certificate
AccessControlBroker	a DCC Access Control Broker Certificate
transitionalCoS	a DCC CoS Certificate
Supplier	one of the following: a. one of the relevant Supplier Party's Organisation Certificates; b. a DCC Access Control Broker Certificate; c. (where the consent of that other Supplier Party has been given) one of that other Supplier Party's Organisation Certificates.
networkOperator	one of the following: a. one of the relevant Network Operator's Organisation Certificates; b. one of the relevant Supplier Party's Organisation Certificates; c. (where the consent of that other Supplier Party has been given) one of that other Supplier Party's Organisation Certificates; d. a DCC Access Control Broker Certificate.
wanProvider	a DCC WAN Provider Certificate
loadController	one of the following: a. one of the relevant Supplier Party's Organisation Certificates; b. a DCC Access Control Broker Certificate; c. (where the consent of that other Supplier Party has been given) one of that other Supplier Party's Organisation Certificates.

Where 'DCC Recovery Certificate', 'DCC CoS Certificate', 'DCC Access Control Broker Certificate' and 'DCC WAN Provider Certificate' are each Organisation Certificates created by the DCC for the purposes of occupying the relevant Trust Anchor Cells on Devices in accordance with the above table and used by those

DCC Systems described in (respectively) sub-paragraphs (f), (c), (b) and (a) of the definition of DCC Live Systems.

3.3 Where and to the extent that the Electricity Distributor or Gas Transporter for a SMETS2+ Device has notified the Responsible Supplier for the Device of the values for the 'NP Configurable Data Items' that the Electricity Distributor or Gas Transporter (as applicable) wishes to have configured on the Device at the time of its Commissioning, the Responsible Supplier shall take all reasonable steps to ensure that those data items are so configured on the Device at the time of its Commissioning, including where the Device is a Standalone Auxiliary Proportional Controller, those items which are both included in the ‘NP Configurable Data Items’ and are supported by the Device. In this Clause 3.3, 'NP Configurable Data Items' means those data items held on Devices that are capable of being configured via Services Requests for which the User Role of 'Electricity Distributors' or 'Gas Transporter' (as applicable) is an Eligible User Role.

Pre-Commissioning obligations in relation to SMETS1 Devices

3.4 Prior to adding a SMETS1 Device (other than a SMETS1 IHD, SMETS1 PPMID or a SMETS1 CAD) to the Smart Metering Inventory, the relevant User shall contact the Service Desk to provide the following information in relation to the Device:

(a) the Device ID; and

(b) any information the DCC reasonably requires in relation to SMETS1 Devices of that Device's Device Model (as made available by the DCC from time to time via the Self-Service Interface).

3.5 The DCC shall not add a SMETS1 Device (other than a SMETS1 IHD or a SMETS1 PPMID) to the Smart Metering Inventory in circumstances where it has not been provided with the information referred to in Clause 3.4 in relation to that Device.

3.6 Where a User has notified the DCC of the Device’s details for recording in the Smart Metering Inventory, before attempting to communicate with the Device via the DCC, the User shall comply with the provisions of Clause 13.1 of the SMETS1 Supporting Requirements.

4. Commissioning

Commissioning of Communications Hub Functions

4.1 Subject to Clause 4.2, where the DCC receives a communication originating from a Communications Hub Function which does not have an SMI Status of 'commissioned' confirming that it has connected to the SM WAN, the DCC shall update the SMI Status of that Communications Hub Function to 'commissioned'.

4.2 Before taking the step set out in Clause 4.1, the DCC shall confirm whether the communication originates from the Communications Hub Function that is identified within the communication. The DCC shall not take the step set out in Clause 4.1 in respect of a Communications Hub Function where:

(a) the Communications Hub Function is not listed within the Smart Metering Inventory;

(b) the Communications Hub Function is not identified in the Smart Metering Inventory as having an SMI Status of 'pending' or 'installed not commissioned'; and/or

(c) the communication may have changed in transit or does not originate from the Communications Hub Function that is identified within the communication.

Adding Devices to Communication Hub Functions' Device Logs

4.3 Following the Successful Execution of an 'Update HAN Device Log' Service Request requesting the addition of a Device to the Device Log of a Communications Hub Function, the DCC shall:

(a) update the Smart Metering Inventory to Associate the Device with the applicable Communications Hub Function;

(b) in the case of Smart Meters and Standalone Auxiliary Proportional Controllers only, record the MPAN(s) or MPRN (as applicable) provided within the Service Request against that Device and notify the Electricity Distributor or Gas Transporter (as applicable) of the MPAN(s) and/or MPRN and of the Device's Device ID and Device Type; and

(c) other than in the case of a Type 2 Device, set the SMI Status of the Device to 'whitelisted'.

4.4 Following the receipt of an Alert from a Communications Hub Function informing the DCC that the Communications Hub Function is able to communicate over the HAN with a Device, the DCC shall (other than in the case of a Type 2 Device, or where the relevant Device already has an SMI Status of 'commissioned') set the SMI Status of the Device to 'installed not commissioned'.

Joining Devices to Smart Meters, Standalone Auxiliary Proportional Controllers or Gas Proxy Functions

4.5 Where a Responsible Supplier wishes to join any Device (other than a Type 2 Device) to a Smart Meter, a Standalone Auxiliary Proportional Controller or a Gas Proxy Function, the Responsible Supplier shall send the DCC a 'Join Service' Service Request to add the relevant Device to the Device Log of the relevant Smart Meter, Standalone Auxiliary Proportional Controller or Gas Proxy Function.

4.6 The DCC shall not send a Command to join a Device to a Smart Meter, Standalone Auxiliary Proportional Controller or Gas Proxy Function in response to a Service Request under Clause 4.5 where:

(a) the Device to be joined is not listed within the Smart Metering Inventory with an SMI Status of 'pending', 'installed not commissioned' or 'commissioned';

(b) the Communications Hub Function that is to form part of the same Smart Metering System is not listed in the Smart Metering Inventory with an SMI Status of 'pending', 'installed not commissioned' or 'commissioned'; and/or

(c) the Smart Meter, Standalone Auxiliary Proportional Controller or Gas Proxy Function with which the Device is to be joined is not listed in the Smart Metering Inventory with an SMI Status of 'pending', 'installed not commissioned' or 'commissioned'.

4.7 On the Successful Execution of a 'Join Service' Service Request to add a Device to the Device Log of a Smart Meter, Standalone Auxiliary Proportional Controller or Gas Proxy Function in accordance with Clauses 4.5 and 4.6, the DCC shall Associate that Device with the applicable Smart Meter, Standalone Auxiliary Proportional Controller or Gas Proxy Function (as applicable), and either:

(a) where the Smart Meter, Standalone Auxiliary Proportional Controller or Gas Proxy Function (as applicable) has an SMI Status of 'installed not commissioned', set the SMI Status of the Device to 'installed not commissioned'; or

(b) where the Smart Meter, Standalone Auxiliary Proportional Controller or Gas Proxy Function (as applicable) has an SMI Status of 'commissioned', set the SMI Status of the Device to 'commissioned'.

4.8 In respect of Type 2 Devices:

(a) where the Responsible Supplier or an Other User wishes to add a Type 2 Device to the Device Log of an Electricity Smart Meter, a Standalone Auxiliary Proportional Controller or a Gas Proxy Function, it shall send a 'Join Service' Service Request in order to do so;

(b) the DCC shall not send a Command to join a Type 2 Device to a Smart Meter, Standalone Auxiliary Proportional Controller or Gas Proxy Function in response to a Service Request under Clause 4.8(a) where the Electricity Smart Meter or Standalone Auxiliary Proportional Controller or Gas Proxy Function with which the Type 2 Device is to be Associated is not listed in the Smart Metering Inventory with an SMI Status of 'pending', 'installed not commissioned' or 'commissioned'; and

(c) on the Successful Execution of a 'Join Service' Service Request to add a Type 2 Device to the Device Log of a Smart Meter, Standalone Auxiliary Proportional Controller or Gas Proxy Function in accordance with (a) and (b) above, the DCC shall Associate that Device with the applicable Smart Meter, Standalone Auxiliary Proportional Controller or Gas Proxy Function (as applicable).

Commissioning of Devices other than Communications Hub Functions

4.9 Where a Responsible Supplier wishes to Commission a Type 1 Device, it shall send (under Clause 4.5) a 'Join Service' Service Request to add the Type 1 Device to the Device Log of a Commissioned Electricity Smart Meter, a Commissioned Standalone Auxiliary Proportional Controller or a Commissioned Gas Proxy Function (as applicable).

4.10 Where a Responsible Supplier wishes to Commission a Gas Proxy Function, it shall send (under Clause 4.5) a 'Join Service' Service Request to add the Gas Proxy Function to the Device Log of a Commissioned Gas Smart Meter.

4.11 Where a Responsible Supplier wishes to Commission a Smart Meter or Standalone Auxiliary Proportional Controller, the Responsible Supplier shall send the DCC a 'Commission Device' Service Request in respect of that Device.

4.12 The DCC shall not send a Command to a Device in response to a Service Request under Clause 4.11 where:

(a) the Device is not listed within the Smart Metering Inventory;

(b) the Device has an SMI Status of 'commissioned', 'decommissioned' or 'suspended'; and/or

(c) the Communications Hub Function that is to form part of the same Smart Metering System is not listed in the Smart Metering Inventory with an SMI Status of 'commissioned'.

4.13 Following the receipt of a Response, over the SM WAN, that indicates the Successful Execution of a 'Commission Device' Service Request in accordance with Clauses 4.11 and 4.12 in respect of a Device, the DCC shall update the SMI Status of the Device to 'commissioned'.

4.14 In respect of SMETS2+ Devices only, as soon as reasonably practicable after the Successful Execution of a 'Commission Device' Service Request which relates to a Smart Meter, the Responsible Supplier shall send a 'Set Device Configuration (Import MPxN)' Service Request to ensure that the relevant MPAN or MPRN (as applicable) is available for display upon the Smart Meter.

4.15 For the avoidance of doubt, there is no concept of commissioning a Type 2 Device.

4.16 Where, following the fitting and activation procedure, the installing Supplier Party wishes to leave a Smart Metering System installed without establishing a connection to the SM WAN, then following any subsequent change of supplier:

(a) the gaining Supplier Party may contact the losing Supplier Party (and/or one or more former suppliers) by email requesting the installation codes for the Devices which comprise that Smart Metering System; and

(b) the installing Supplier Party shall, within ten (10) Working Days of receiving such a request, provide the relevant installation codes to the gaining Supplier Party by email (or, if the Supplier Party which is contacted is not the installing Supplier Party, confirm the same to the gaining Supplier Party by email).

5. Post-Commissioning Obligations in relation to SMETS2+ Devices

5.1 This Clause 5 applies only to SMETS2+ Devices.

5.2 As soon as reasonably practicable (and in any event within 7 days) following the Commissioning of a Communications Hub Function, the DCC shall ensure that:

(a) the Communications Hub Function re-generates its Private Keys, and that Device Certificates containing the associated new Public Keys are stored on the Device; and

(b) the information from at least one of the Organisation Certificates that comprise the Communications Hub Function's Device Security Credentials is replaced (provided that for such purposes the information from an Organisation Certificate may be replaced with that from the same Organisation Certificate).

5.3 As soon as reasonably practicable (and in any event within 7 days) following the Commissioning of a Smart Meter, a Standalone Auxiliary Proportional Controller or a Gas Proxy Function, the Responsible Supplier shall, in relation to each such Device, ensure that:

(a) the Device Security Credentials which pertain to the Network Parties are:

(i) in the case of those which pertain to the Electricity Network Party, those of the Electricity Distributor; and

(ii) in the case of those which pertain to the Gas Network Party, those of the Gas Transporter (or, if they are not available in the SMKI Repository, the Device Security Credentials which pertain to the Gas Network Party shall be populated with information from the Organisation Certificates Issued to the DCC and referred to in Sections L3.23(f) (the DCC (access-Control-Broker) – digitalSignature Certificate) and L3.23(g) (the DCC (access-Control-Broker) – keyAgreement Certificate));

(b) the Device re-generates its Private Keys, and that the Device Certificates containing the associated new Public Keys are stored on the Device; and

(c) in the case of a Smart Meter and a Standalone Auxiliary Proportional Controller, information from at least one of the Organisation Certificates that comprise the Device's Device Security Credentials is replaced (provided that for such purposes the information from an Organisation Certificate may be replaced with that from the same Organisation Certificate).

5.4 As soon as reasonably practicable (and in any event within 7 days) following the Commissioning of a Communications Hub Function, Gas Proxy Function, Standalone Auxiliary Proportional Controller or Smart Meter, the DCC shall interrogate the Device to ascertain whether the Device's recovery Trust Anchor Cell is populated with Device Security Credentials that pertain to a DCC Recovery Certificate. For Devices Commissioned before Service Release 1.3 (or such later date as may be directed by the SofS for the purposes of this Clause 5.4), the reference to the period of 7 days following Commissioning shall apply as 7 days following Service Release 1.3 (or 7 days following any later date directed by the SofS).

5.5 The DCC shall monitor Commands sent to Devices and the associated Responses from Devices and, based on the information available to it, record the information set out in Clause 5.8 in relation to each Device identified in Clause 5.7 (the "**Post Commissioning Information**").

5.6 The DCC shall ensure that the Post Commissioning Information is updated on a daily basis to reflect the most accurate and up-to-date information available to the DCC at the time of the update.

5.7 For the purposes of Clause 5.5, the relevant Devices include any Communications Hub Function, Gas Proxy Function, a Standalone Auxiliary Proportional Controller or Smart Meter which has an SMI Status of 'commissioned', has been Commissioned for a period of 7 days or more, and in relation to which one or both of the following applies:

(a) the DCC has failed successfully to carry out the interrogation of the Device pursuant to Clause 5.4; and/or

(b) the DCC has successfully carried out the interrogation of the Device pursuant to Clause 5.4 and has identified that the Device's recovery Trust Anchor Cell is not populated with Device Security Credentials that pertain to a DCC Recovery Certificate.

5.8 For the purposes of Clause 5.5, the Post Commissioning Information to be recorded in relation to each relevant Device shall include:

(a) the Device ID and Device Type;

(b) the date upon which the Device was Commissioned;

(c) which of Clauses 5.7 (a) and/or (b) applies;

(d) other than in the case of Communications Hub Functions, the Responsible Supplier at the time the Post Commissioning Information for the Device was most recently updated;

(e) other than in the case of Communications Hub Functions, the Supplier Party that sent the Service Request that resulted in the Commissioning of the Device; and

(f) the date on which the Post Commissioning Information for the Device was most recently updated.

5.9 As soon as reasonably practicable following the end of each month, the DCC shall, based upon the Post Commissioning Information prevailing at the end of that month, compile and provide (in an electronic format) to the Panel, the Security Sub-Committee and the Authority a report which includes the following information:

(a) the month to which the report relates;

(b) for each Party that is the Responsible Supplier for any Smart Meter or Gas Proxy Function that is listed in the Post Commissioning Information for that month (or was listed in the information for the previous month):

(i) the total number of Devices of each Device Type listed in the Post Commissioning Information for that month for which that Party is the Responsible Supplier;

(ii) the number of such Devices of each Device Type that have been added since the last monthly report;

(iii) the number of such Devices of each Device Type that have been removed since the last monthly report;

(iv) the number of such Devices of each Device Type that were listed in the Post Commissioning Information for the previous month and remain listed in the information for the month to which the report relates;

(v) the number of such Devices of each Device Type that were listed in the Post Commissioning Information for the previous three months and remain listed in the information for the month to which the report relates; and

(vi) the number of such Devices of each Device Type that were listed in the Post Commissioning Information for the previous six months and remain listed in the information for the month to which the report relates; and

(c) in respect of Communications Hub Functions:

(i) the total number of Communications Hub Functions listed in the Post Commissioning Information;

(ii) the number of Communications Hub Functions that have been added since the last monthly report;

(iii) the number of Communications Hub Functions that have been removed since the last monthly report;

(iv) the number of Communications Hub Functions that were listed in the Post Commissioning Information for the previous month and remain listed in the information for the month to which the report relates;

(v) the number of Communications Hub Functions that were listed in the Post Commissioning Information for the previous three months and remain listed in the information for the month to which the report relates; and

(vi) the number of Communications Hub Functions that were listed in the Post Commissioning Information for the previous six months and remain listed in the information for the month to which the report relates.

5.10 As soon as reasonably practicable following the end of each day, the DCC shall, based upon the Post Commissioning Information prevailing at the end of that day, compile and make available to each Supplier Party (via a secure electronic means for a period of at least 30 days following the day to which the report relates) a report which includes the following information in relation to Devices (other than Communications Hub Functions) listed in the Post Commissioning Information for which that Supplier Party was the Responsible Supplier on that day:

(a) the Device ID and Device Type of each such Device;

(b) the date on which the Post Commissioning Information for each such Device was most recently updated;

(c) the date upon which each such Device was Commissioned; and

(d) which of Clause 5.7 (a) and/or (b) applies in relation to each such Device.

5.11 Where requested by the Panel or the Authority, the DCC shall, as soon as reasonably practicable following any such request, provide to the Panel and/or the Authority (in an electronic format) copies of the reports referred to in Clause 5.10. Where requested by the Panel or the Authority, DCC shall additionally include in any such report the information referred to in Clause 5.8(e) in relation to each Device included in any such report.

5.12 The DCC shall ensure that each report provided under Clause 5.9, 5.10 or 5.11 is clearly marked as being "confidential".

5.13 Where the DCC is aware that:

(a) either or both of the steps in Clauses 5.2 (a) and/or (b) have not been carried out within 7 days following the Commissioning of a Communications Hub Function; and/or

(b) either of Clause 5.7(a) or (b) applies in relation to a Communications Hub Function,

then the DCC shall raise an Incident in accordance with the Incident Management Policy.

5.14 Where, in relation to a Gas Proxy Function, Standalone Auxiliary Proportional Controller or a Smart Meter, a Supplier Party is aware that:

(a) either or both of the steps in Clauses 5.3 (b) and/or (in the case of Smart Meters and Standalone Auxiliary Proportional Controllers only) 5.3(c) have not been carried out within 7 days following the Commissioning of the Device; and/or

(b) the DCC has failed successfully to carry out the interrogation of the Device pursuant to Clause 5.4, and the Supplier has (within a period of 14 days following the Commissioning of the Device) also failed to successfully carry out the relevant interrogation,

then the Supplier Party shall not send Service Requests requesting that the DCC sends communications to that Device other than for the purposes of: (i) completing those steps; (ii) replacing the Device Security Credentials held on the Device in response to a change of supplier; or (iii) maintaining an energy supply to the relevant premises.

5.15 Where the Responsible Supplier for a Gas Proxy Function, Standalone Auxiliary Proportional Controller or Smart Meter becomes aware that the Device does not have a recovery Trust Anchor Cell that is populated with Device Security Credentials that pertain to a DCC Recovery Certificate, then that Responsible Supplier shall (subject to Clause 5.17), as soon as reasonably practicable thereafter: other than in the case of a Gas Proxy Function, replace the Device; or, in the case of a Gas Proxy Function, replace the Communications Hub of which that Gas Proxy Function forms part.

5.16 Where a Communications Hub is returned to the DCC:

(a) following its replacement pursuant to Clause 5.13 or 5.15; or

(b) a Communications Hub is returned following replacement because it was not possible to interrogate the Gas Proxy Function pursuant to Clause 5.14(b),

then the Supplier Party returning the Communications Hub may (under and subject to Section F9 (Categories of Communications Hub Responsibility)) specify the reason for return as being a CH Defect.

5.17 A Responsible Supplier shall not replace a Device under Clause 5.15 where the reason that the relevant steps cannot be completed is an inability to communicate with a Device as a result of the SM WAN being unavailable.

General Obligations on DCC

5.18 The DCC shall monitor Responses it receives from Devices in order to determine whether any of the Device Certificates held on each Device have been successfully replaced. On the basis of this information the DCC shall establish and maintain a record of the most up-to-date active Device Certificates for each Device.

5.19 Where, following the addition of a Device to the Device Log of a Communications Hub Function, the DCC identifies that a Trust Anchor Cell of that Device has been populated with Security Credentials derived from a DCC CoS Certificate that has a subject field that is populated with an identifier of a DCC Service Provider that does not provide services to the CoS Party, the DCC shall send a DCC Alert to the Responsible Supplier for the Device, notifying them of the situation.

6. Post-Commissioning Obligations in relation to SMETS1 Devices

6.1 This Clause 6 applies only to SMETS1 Devices.

6.2 As soon as reasonably practicable (and in any event within 7 days) following the Commissioning of a SMETS1 Device, the Responsible Supplier shall ensure that:

(a) the Device Security Credentials which pertain to the Responsible Supplier are those of the Import Supplier or Gas Supplier (as applicable);

(b) the Device Security Credentials which pertain to the Electricity Network Party are those of the Electricity Distributor; and

(c) the Device Security Credentials which pertain to the Gas Network Party are those of the Gas Transporter (or, if they are not available in the SMKI Repository, the Device Security Credentials which pertain to the Gas Network Party shall be populated with information from the Organisation Certificates Issued to the DCC and referred to in Sections L3.23(f) (the DCC (access-Control-Broker) – digitalSignature Certificate) and L3.23(g) (the DCC (access-Control-Broker) – keyAgreement Certificate)).

6.3 Where any Party takes an action that results in a change to the information provided under Clause 3.4 it must (prior to doing so, or as soon as reasonably practicable thereafter) contact the Service Desk and notify the DCC of the updated information.

6.4 Where a Responsible Supplier for a SMETS1 CHF replaces the Device (or any component part of the Device that affects the means by which the DCC communicates with it), the Responsible Supplier must ensure that the replacement Device (or replacement parts) are such that that the DCC remains capable of communicating with that Device (where necessary after updating the information referred to in Clause 6.3 in relation to that Device).

6.5 As soon as reasonably practicable (and in any event within 7 days) following the Commissioning of a SMETS1 Device and thereafter at the frequency specified in the SMETS1 Supporting Requirements for the relevant Device Model, the DCC shall ensure that the Private Keys and / or Symmetric Keys, identified as being required by the SMETS1 Supporting Requirements to be replaced for such Device Models, are so replaced.

7. Unjoining

7.1 In the case of any Device other than a Standalone Auxiliary Proportional Controller or a Smart Meter, on the Successful Execution of an 'UnJoin Service' Service Request to remove that Device from the Device Log of an other Device, the DCC shall terminate the Association between that Device and the other Device.

8. Reactivating Decommissioned or Suspended Devices

8.1 Where the Responsible Supplier wishes to change the SMI Status of any Device (other than a Type 2 Device) from 'decommissioned' or 'whitelisted' to 'pending', then the Responsible Supplier shall send the DCC a Service Request to that effect. Provided the Device in question is of (or is part of) a Device Model that is identified in the Central Products List, the DCC shall change the SMI Status to 'pending'.

8.2 Where the SMI Status of a Device has remained as 'pending' for 36 months, then the DCC shall remove the Device from the Smart Metering Inventory.

8.3 Where a Device ceases to be Suspended (either as a result of the Device Model being added to the Central Product List, or the Device's Device Model being modified such that it is on the Central Product List), the DCC shall change the SMI Status of that Device to the status it held immediately prior to its Suspension.

9. Replacement of SMETS2+ Communications Hub Functions

9.1 This Clause 9 only applies to SMETS2+ Devices.

9.2 The DCC shall monitor Alerts and Responses sent from each Communications Hub Function and Gas Proxy Function in order to establish and maintain an up-to-date electronic record of the most recent information stored in the Device Log of each such Device.

9.3 Where DCC receives a 'Restore HAN Device Log' or 'Restore Gas Proxy Function Device Log' Service Request, the DCC shall use the up-to-date electronic record referred to in Clause 9.2 in relation to the relevant Device for the purposes of determining the information to be used to restore the Device Log of the relevant Device.

9.4 Where a Communications Hub is replaced and the Communications Hub Function and Gas Proxy Function that comprise the replacement Communications Hub are Commissioned, such Devices shall (for the avoidance of doubt) be considered to be newly Commissioned and any provisions of the Code which require steps to be taken by any Party in relation to a newly Commissioned Device shall apply.

10. Removal of SMETS1 Communications Hub

10.1 Where practicable, prior to, and if not as soon as possible after, removing a SMETS1 Communications Hub, the Lead Supplier for that Communications Hub shall ensure the SMI Status for the relevant SMETS1 CHF is set to ‘decommissioned’.

11. Notification of Decommissioning and Suspension of Devices

11.1 As soon as reasonably practicable following the Decommissioning or Suspension of a Smart Meter or Standalone Auxiliary Proportional Controller, the DCC shall notify the Electricity Distributor or Gas

Transporter for that Device of such Decommissioning or Suspension, such notification to be made via the DCC User Interface.

11.2 As soon as reasonably practicable following the Suspension of a Device, the DCC shall notify the Responsible Supplier(s) for that Device of such Suspension, such notification to be made via the DCC User Interface.

12. CH Production Proving

12.1 The purpose of CH Production Proving is to provide assurance on the operation of the DCC Total System.

12.2 CH Production Proving entails the Commissioning of Communications Hub Functions and the sending and receiving of communications by the DCC to and from those Communications Hub Functions over the SM WAN. CH Production Proving is to be undertaken within the DCC Live Systems.

12.3 In order that the DCC can undertake CH Production Proving using particular Communications Hub Functions, those Communications Hub Functions will need to be included within the Smart Metering Inventory. The DCC shall only be entitled to include Communications Hub Functions (and the associated Gas Proxy Functions) within the Smart Metering Inventory for the purpose of CH Production Proving where the Security Sub-Committee has approved the inclusion of those Communications Hub Functions (and the associated Gas Proxy Functions) for such purpose.

12.4 The DCC shall, from time to time, be entitled to undertake CH Production Proving (and the other provisions of this Code shall be interpreted accordingly).

12.5 The DCC shall undertake CH Production Proving in accordance with Good Industry Practice, in a manner that does not adversely affect the provision of the Services, and in accordance with any conditions imposed by the Security Sub-Committee in respect of its approval pursuant to Clause 12.3.

13. Definitions

13.1 For the purposes of this Appendix:

(a) "**Trust Anchor Cell**", in relation to any Device, has the meaning given to it in the GB Companion Specification;

(b) "**keyUsage**", in relation to any Certificate, means the field referred to as such in the Organisation Certificate Policy;

(c) "**Service Release 1.3**" means, where the Secretary of State makes directions pursuant to Section X3 (Provisions to Become Effective Following Designation) whereby the DCC User Interface Services Schedule is varied on it first becoming effective so that there are Service Requests that are deemed to be omitted from the document, the date on which one or more of those variations are cancelled; and

(d) "**CH Production Proving**" is the activity described in Clause 12.

Appendix AD – DCC USER INTERFACE SPECIFICATION

[Please use this placeholder to download your required version of SEC Appendix AD 'DCC User Interface Specification']

Download SEC Appendix AD 'DCC User Interface Specification' version 1.1 here.

Download SEC Appendix AD 'DCC User Interface Specification' version 2.0 here.

Download SEC Appendix AD 'DCC User Interface Specification' version 3.0 here.

Download SEC Appendix AD 'DCC User Interface Specification' version 3.1 here.

Download SEC Appendix AD 'DCC User Interface Specification' version 4.0 here.

Download SEC Appendix AD 'DCC User Interface Specification' version 5.0 here.

Download SEC Appendix AD 'DCC User Interface Specification' version 5.1 here.

Download SEC Appendix AD 'DCC User Interface Specification' version 5.2 here.

Version AE 1.0

APPENDIX AE

DCC User Interface Code of Connection

DEFINITIONS

DUIS XML Schema	has the meaning set out in the DCC User Interface Specification.
Receive Response Service	has the meaning set out in the DCC User Interface Specification.
Security Patch	has the meaning set out in the Registration Data Interface Code of Connection.
Transport Layer Security (TLS)	has the meaning set out in the DCC User Interface Specification.

1. DCC USER INTERFACE CODE OF CONNECTION

1.1 These provisions apply to the DCC and any User seeking to send or receive the communications listed in Section H3.3.

General Obligations

1.2 The DCC and each User shall inform each other of the contact details of one or more persons working for their respective organisations for the purposes of managing arrangements associated with the use of the DCC User Interface. The following information shall be provided in relation to each such person (and subsequently kept up to date by the User or the DCC):

(a) contact name;

(b) contact email;

(c) contact telephone number; and

(d) contact address.

and any other contact details as may be reasonably required by the DCC or the User from time to time.

Restrictions on Access to DCC User Interface

1.3 Each User shall only access the DCC User Interface via a DCC Gateway Connection.

Establishment of Transport Layer Security

1.4 The DCC and each User:

(a) shall establish a TLS session to secure the transport layer connection to the User’s Receive Response Service or the DCC User Interface respectively and shall do so in accordance with the DCC User Interface Specification;

(b) shall use a DCCKI Infrastructure Certificate to establish the TLS session; and

(c) in the case of a User only, may obtain a DCCKI Infrastructure Certificate in accordance with the DCCKI RAPP.

Technical Infrastructure

1.5 Each User shall only send Service Requests or Signed Pre-Commands where they have successfully validated those Service Requests or Signed Pre-Commands against the DUIS XML Schema.

1.6 Each User shall inform the DCC of the following information relating to its Receive Response Service in relation to any DCC Gateway Connection that it is using to access the DCC User Interface:

(a) primary URL and/or IP address for its Receive Response Service; and

(b) alternate URL and/or IP address for its Receive Response Service (if required for secondary location).

and shall inform the DCC if there are any changes to such information.

1.7 Each User shall provide the DCC with reasonable advance notice of any expected outages in the availability of its Receive Response Service that may impact the DCC's ability to send information to the User.

1.8 The DCC shall ensure that the URL and/or the IP address of the DCC User Interface remain constant.

1.9 The DCC shall use UTC (Coordinated Universal Time) for all messages sent over the DCC User Interface.

Security Obligations

1.10 Each User shall test the installation of Security Patches to be applied to its User Systems prior to their application.

1.11 Prior to first using the DCC User Interface, each User shall provide a report to the DCC that details the following:

(a) the scope of its User Systems;

(b) the number of connections between its User Systems and any system that does not form part of the User Systems; and

(c) the means by which the User has achieved Separation between its User Systems and each other system to which they connect.

and;

thereafter, the User shall ensure that the DCC is provided with a revised report whenever there is a change to the underlying information used to compile its previous report.

1.12 Where the DCC considers that:

(a). the User Systems are at risk of Compromise as a consequence of one or more features of a System which has not been Separated from (and therefore forms part of) those User Systems; and

(b). the User Systems are at risk of Compromise to such an extent that the User is likely to be non-compliant with Section G; and (c). that risk of Compromise (and therefore of non-compliance with Section G) could be appropriately mitigated by means of the Separation of the System which gives rise to the risk from the other Systems which are comprised in the User Systems; and

(d). that the non-compliance with Section G poses a threat of Compromise of DCC Systems,

the DCC shall notify the User and the Panel and provide an associated explanation.

Appendix AF – Message Mapping Catalogue

[Please use this placeholder to download your required version of SEC Appendix AF 'Message Mapping Catalogue']

Download SEC Appendix AF 'Message Mapping Catalogue' version 1.0 here.

Download SEC Appendix AF 'Message Mapping Catalogue' version 2.0 here.

Download SEC Appendix AF 'Message Mapping Catalogue' version 3.0 here.

Download SEC Appendix AF 'Message Mapping Catalogue' version 3.1 here.

Download SEC Appendix AF 'Message Mapping Catalogue' version 4.0 here.

Download SEC Appendix AF 'Message Mapping Catalogue' version 5.0 here.

Download SEC Appendix AF 'Message Mapping Catalogue' version 5.1 here.

Download SEC Appendix AF 'Message Mapping Catalogue' version 5.2 here.

Version AG 6.0

Appendix AG

Incident Management Policy

Contents

Definitions

In this document, except where the context otherwise requires:

- Expressions defined in section A of the Code (Definitions and Interpretation) have the same meaning as is set out in that section;
- The expressions in the left hand column below shall have the meaning given to them in the right hand column below; and
- References throughout to Service Desk mean the DCC via the Service Desk.

Business Continuity Event	An Event, other than a Disaster, that causes one or more of the 'DCC BC Impacts' listed in Table 4 of this document.
CPNI	Centre for the Protection of National Infrastructure
Code of Connection	One of the following Subsidiary Documents: DCC Gateway Connection Code of Connection; DCC User Interface Code of Connection; Registration Data Interface Code of Connection; Self-Service Interface Code of Connection; SMKI Code of Connection; SMKI Repository Code of Connection; DCCKI Code of Connection; DCCKI Repository Code of Connection.
Error Handling Strategy	The procedures to be followed and actions to be taken where a Service Request or the commands or responses related to it fail to provide the result expected from that type or category of Service Request as further described in clause 4
HMG	Her Majesty's Government
Interested Party	A Party or Registration Data Provider that is or has the potential to be affected by a Problem or Incident
Known Error	A fault in a component of the DCC Total System which is used for the provision of Live Services, identified by the successful diagnosis of an Incident or Problem and for which both Root Cause and a temporary work-around or a permanent solution have been identified

Live Service	Means 1) any of the Services that the DCC is obliged to provide to a User, an Authorised Subscriber, a DCC Gateway Party (once its connection is capable of operation), but excluding Testing Services as set out in H14, and 2) the exchange of data pursuant to Section E2.
Nominated Individual	means an individual who has been nominated by an Incident Party in accordance with clause 1.4.5 of this Incident Management Policy
Normal Business Day	means the period starting 08:00 and finishing at 18:00 on a Working Day.
Normal Business Hours	means hours during a Normal Business Day.
Root Cause	is the ultimate cause of an Incident or Problem
Root Cause Analysis	a class of problem solving methods aimed at identifying the Root Cause of a Problem or Incident
Service Alert	An alert notifying Interested Parties of a current issue which may impact the provision of Services
Target Initial Response Time	The time period within which an Incident within each Category should be recorded on the Incident Management Log and assigned to a resolver

1. Introduction

1.1. Purpose

1.1.1 This document details the Incident Management Policy in accordance with the requirements of Section H9. It deals with the management of Incidents, including those related to Registration Data.

1.1.2 Additionally, Clauses 4 and 5 cover the Error Handling Strategy and Business Continuity and Disaster Recovery respectively.

1.2. Background

1.2.1 The subject matter of this document is closely related to that of the Incident Management aspects of the Registration Data Interface Specification. In order to ensure an integrated solution to managing Incidents, certain common aspects of Incident Management are set out in this document and cross-referred to in the Registration Data Interface Specification.

1.2.2 The Registration Data Incident types are set out in the Registration Data Interface Specification.

1.2.3 Error conditions and how they should be handled are covered in Clause 4, the Error Handling Strategy.

1.3. Scope

1.3.1 The Incident Management Policy details the full Incident Management lifecycle including management and declaration of Major Incidents, Problems and escalations.

1.4. General Provisions

1.4.1 Incidents may be raised only by the DCC or an Incident Party and in accordance with this Incident Management Policy.

1.4.2 Incidents raised and managed under this Incident Management Policy may relate to any Live Service. The Testing Issue Resolution Process set out in H14.37- H14.45 shall apply for the purpose of resolving Testing Issues.

1.4.3 In the event that an Incident Party considers it necessary to raise an issue relating to the provision of Services but which it considers outside the scope of Live Services or Testing Services, it shall contact the DCC directly and each of that Party and the DCC shall, acting reasonably, agree between them responsibility for resolution of the issue, which shall be resolved by the responsible Party as soon as reasonably practicable.

1.4.4 Incidents shall be raised and recorded in the Incident Management Log in accordance with Clause 2.

1.4.5 Each Incident Party shall provide the DCC with, and shall subsequently provide the DCC with any changes to, a list of Nominated Individuals from their organisation who are authorised to:

(a) contact the DCC to raise and record in the Incident Management Log an Incident and communicate with the DCC regarding the Incident; and/or

(b) perform the roles identified in the escalation process defined in Clause 2.9.

1.4.6 Each Registration Data Provider, when providing the DCC with a list of Nominated Individuals, shall provide details of both the core operating hours for the Registration Data Provider and the Registration Data Provider’s out-of-hours facility.

1.4.7 Each Incident Party shall ensure that only its Nominated Individuals shall contact the DCC to raise an Incident.

1.4.8 The DCC shall ensure that only those Nominated Individuals pursuant to Clause 1.4.5(a) shall raise an Incident.

1.4.9 The DCC shall implement an authentication procedure for confirming that a communication is from an Incident Party’s Nominated Individual, and such procedure shall be commensurate with the risk to the Services and Data that would arise were someone other than a Nominated Individual to raise an Incident or obtain information from the Service Desk. Incident Parties shall comply with this procedure.

1.4.10 The DCC and each Incident Party shall each ensure that information regarding Incidents and Problems is recorded and kept up to date in the Incident Management Log as follows:

(a) for Major Incidents, the Incident Party shall comply with Clause 2.2.2;

(b) except in the case of Clause 1.4.10 (a), the Incident Party shall use the Self-Service Interface where it is able to do so and the DCC shall ensure that information provided in this way is automatically added to the Incident Management Log;

(c) where the Incident Party is unable to use the Self-Service Interface, it shall provide information to the Service Desk by email or by phone and the Service Desk shall ensure that this information is entered into the Incident Management Log;

(d) when an Incident is submitted by email and the Incident Party does not provide the required information as detailed in Clause 2.3, the Service Desk shall return an email to the Incident Party requesting the missing information and the Incident shall not be recorded in the Incident Management Log until the required information has been received by the Service Desk;

(e) the Service Desk shall enter information that the DCC originates into the Incident Management Log;

(f) the resolver shall ensure all actions to resolve the Incident are recorded in the Incident Management Log; and

(g) In regard to items a) – f) above, the DCC and each Incident Party shall each ensure that information is as complete as is possible and is entered into the Incident Management Log as soon as is reasonably practicable.

2. INCIDENT MANAGEMENT

2.1. Pre-requisites to Raising an Incident

DCC

2.1.1 Before raising an Incident the DCC shall take all reasonable steps to ensure an Incident does not already exist for the issue.

2.1.2 Not used.

Incident Parties other than Registration Data Providers

2.1.3 For the purposes of this clause 2.1.3 and clause 2.1.4, references to “Incident Party” do not include Registration Data Providers.

Before raising an Incident with the DCC the Incident Party shall take all reasonable steps to:

(a) where appropriate, confirm that the issue does not reside within the HAN, or the Smart Meter, or other Devices which the Incident Party is responsible for operating;

(b) confirm that the issue does not reside within the Incident Party’s own systems and processes;

(c) follow the guidance set out in the self-help material made available by the DCC, including checking for Known Errors and the application of any workarounds specified; and

(d) where the party is a User and to the extent that this is possible, use the SSI or submit a Service Request to resolve the Incident in accordance with Section H9.2.

2.1.4 In the event that the activities in clause 2.1.3 have been completed and an Incident is to be raised with the DCC, where it has access to the Self-Service Interface, the Incident Party shall check on the Self-Service Interface to establish whether an Incident has already been raised or a Service Alert issued for this issue and:

(a) in the event that the Incident Party can reasonably determine that an Incident or Service Alert for this issue exists, the Incident Party shall notify the Service Desk who shall register the Incident Party as an Interested Party within the Incident Management Log;

(b) in the event that the Incident Party cannot identify an existing Incident or Service Alert they shall progress to clause 2.2 to raise an Incident.

Registration Data Provider

2.1.5 Prior to raising an Incident regarding the provision of data by the DCC, the Registration Data Provider shall take all reasonable steps to confirm that the issue does not reside within the Registration Data Provider’s systems and processes.

2.2. Raising an Incident

2.2.1 Incidents can be raised at any time as set out in in clause 2.2.3, but only once the steps in clause 2.1 have been followed.

2.2.2 Where an Incident Party believes that an Incident meets the criteria of a Category 1 Incident (see clause 2.4.4), the Incident Party shall call the Service Desk as soon as reasonably practicable.

2.2.3 An Incident Party shall raise what it considers to be Category 2, 3, 4 and 5 Incidents as set out in clause 1.4.10 and provide information as set out in clause 2.3.1.

2.3. Required Information

2.3.1 When raising an Incident, the DCC or Incident Party shall provide the following information:

(a) Contact name;

(b) Contact Organisation;

(c) Contact details;

(d) Organisation’s Incident reference number (where available);

(e) Date and time of occurrence;

(f) MPxN or Device ID (where appropriate);

(g) Summary of Incident;

(h) Business impact; and

(i) Results of initial triage and diagnosis including references to existing Incidents, where appropriate, and details of investigations performed to satisfy pre-requisites set out in clause 2.1.

2.4. Incident Prioritisation and Categorisation

2.4.1 The DCC shall assign an Incident Category to an Incident raised by an Incident Party based on the information available at the time the Incident is recorded in the Incident Management Log.

2.4.2 The DCC shall assign an Incident Category to an Incident raised by the DCC using information available to the DCC at the time the Incident is recorded in the Incident Management Log.

2.4.3 The DCC shall progress the resolution of Incidents in priority order. The DCC shall determine the priority of an Incident by considering the Incident Category and the time remaining until the Target Resolution Time, as defined in clause 2.4.4.

Categorisation Matrix

2.4.4 The DCC shall, acting reasonably, assign a Category to an Incident, having regard to the table below. The table further details the Target Resolution Time in accordance with Section H9.1(c). If there is an Incident which is caused in whole or in part by the SMETS1 SM WAN and if Telefonica UK Limited or Vodafone Global Enterprise Limited is the relevant DCC Service Provider then the Target Initial Response Time and Target Resolution Time data set out in the table are non-binding on the DCC.

Incident Category	Description	All Incidents except those caused in whole or in part by the SMETS1 SM WAN if Vodafone Global Enterprise Limited or Telefonica UK Limited is the relevant DCC Service Provider		Incidents caused in whole or in part by the SMETS1 SM WAN if Vodafone Global Enterprise Limited is the relevant DCC Service Provider		Incidents caused in whole or in part by the SMETS1 SM WAN if Telefonica UK Limited is the relevant DCC Service Provider	
		Target Initial Response Time	Target Resolution Time	Target Initial Response Time	Target Resolution Time	Target Initial Response Time	Target Resolution Time
1	A Category 1 Incident (Major Incident) is an Incident which, in the reasonable opinion of the DCC: • prevents a large group of Incident Parties from using the Live Services; • has a critical adverse impact on the activities of the Incident Parties using the Live Services of the DCC; • causes significant financial loss and/or disruption to the Incident Parties; or • results in any material loss or	10 minutes	4 hours	N/A	7 hours	2 hours	5 hours

	corruption of DCC Data. For a Major Security Incident there are additional considerations: • HMG, through CPNI, have declared a Major Incident based on their procedures; • a pattern has been seen across the DCC Total System that in total would have a significant security impact; or • Data covered by the Data Protection Act has either been lost or obtained by an unauthorised party, or is seriously threatened.						
2	An Incident which in the reasonable opinion of the DCC: • has a non-critical adverse impact on the activities of Incident Parties, but the Live Service is still working at a reduced capacity; or • causes financial loss and/or disruption to other Incident Parties which is more than trivial but less severe than the significant financial loss described in the definition of a	20 minutes	24 hours	N/A	17 hours	4 Normal Business Hours or 2 hours if raised outside a Normal Business Day	12 Normal Business Hours or 5 hours if raised outside a Normal Business Day

	Category 1 Incident.						
3	An Incident which, in the reasonable opinion of the DCC: • has an adverse impact on the activities of an Incident Party but which can be reduced to a moderate adverse impact due to the availability of a workaround; or • has a moderate adverse impact on the activities of an Incident Party.	45 minutes	72 hours	N/A	17 hours	9 Normal Business Hours	48 Normal Business Hours
4	An Incident which, in the reasonable opinion of the DCC has a minor adverse impact on the activities of an Incident Party.	3 hours	5 days	N/A	9 days	9 Normal Business Hours	48 Normal Business Hours
5	An Incident which, in the reasonable opinion of the DCC has minimal impact on the activities of Incident Party.	1 day	10 days	N/A	9 days	90 Normal Business Hours	90 Normal Business Hours

Table 1 - This table covers all Incident categories including Security Incidents.

2.4.5 If an Incident Party believes an Incident has been allocated an incorrect Incident Category by the DCC or has been subsequently updated to an incorrect Incident Category by the DCC, it may invoke the escalation process set out in clause 2.9.

2.4.6 The DCC may change the Incident Category of an Incident if more information becomes available. The DCC shall provide to Interested Parties, through a Nominated Individual, details of why the Incident Category has been changed. The DCC shall update the Incident Management Log with the revised Incident Category.

2.5. Incident Assignment

2.5.1 The Service Desk shall manage Incidents recorded in the Incident Management Log through the Incident lifecycle.

2.5.2 The Service Desk shall assess the Incident and assign resolution activities to the appropriate resolver in accordance with Section H9.2, and the resolver may be the DCC or an Incident Party.

2.5.3 In the event that Incident resolution activities are assigned to a Registration Data Provider at a time which falls outside of the Registration Data Provider's hours of operation, and where the DCC has classified the Incident as a Category 1 or 2, the DCC shall contact the Registration Data Provider via its out-of-hours facility as provided in accordance with the clause 1.4.6.

2.5.4 In the event that Incident resolution activities are assigned to a Registration Data Provider at a time which falls outside of the Registration Data Provider's hours of operation and the DCC has classified the Incident as a Category 3, 4 or 5, the DCC shall contact the Registration Data Provider when their business operations commence on the next Working Day. In such instances the time during which the Registration Data Provider was not able to be contacted shall be disregarded for the purpose of calculating the resolution time for the Incident.

2.5.5 Pursuant to H9.8 the resolver assigned to an Incident shall perform the appropriate steps to resolve the Incident in accordance with Section H9.8, and shall record information as set out in clause 1.4.10.

2.5.6 When assigning an Incident to an Incident Party where the DCC requires the Incident Party to diagnose or confirm resolution of an Incident, the DCC shall:

(a) engage with the Incident Party through a Nominated Individual;

(b) set the Incident status to pending; and

(c) assign the activity to the Incident Party, and the resolution time shall not include the period of time during which the Incident is assigned to the Incident Party.

2.5.7 The Incident Party shall, using a reasonable mechanism, confirm to the DCC when all activities requested pursuant to clauses 2.5.5 are complete, providing details of steps taken, which the Service Desk shall ensure are included in the Incident Management Log. The DCC shall then reassign the Incident or update the status in the Incident Management Log to resolved, as appropriate, based on the information received.

2.5.8 Where an Incident has been investigated but has subsequently been determined not to be an Incident:

(a) the Service Desk shall contact the Incident Party that raised the Incident through a Nominated Individual and provide the relevant information that the DCC holds to enable the Incident Party to raise and manage the Incident within its own system; and

(b) the Service Desk shall set the status of the Incident in the Incident Management Log to closed.

2.5.9 If an Incident Party identifies that an Incident has been assigned to it but it should not be responsible for resolving it, the Incident Party shall advise the Service Desk, providing supporting information, and the DCC shall investigate and re-assign as appropriate.

2.5.10 The DCC shall collate and make available to Network Parties and the Panel data related to the time taken to resolve Incidents associated with the exchange of data pursuant to Section E of the Code, where the DCC is responsible for resolving the Incident but in order to do so, activity must be undertaken by a Registration Data Provider.

2.6. Identifying Interested Parties

2.6.1 The Service Desk shall take all reasonable steps using information available from the Live Services including Incident data, as appropriate, to identify Interested Parties for an Incident.

2.6.2 The DCC shall inform the Interested Parties identified by the DCC of the Incident through a Nominated Individual.

2.7. Communications

2.7.1 Throughout the lifecycle of the Incident, the DCC, via the Service Desk, shall communicate updates to the Incident Party or other identified Interested Parties. These communications may be via email, phone call and/or via updates to the Incident Management Log.

2.8. Incident Escalation

2.8.1 The rules and process for the escalation of an Incident are detailed in this clause and clause 2.9.

2.8.2 The DCC and Incident Party shall adopt the escalation process as defined in clause 2.9 to ensure that Nominated Individuals and DCC representatives with the necessary authority and the appropriate resources are applied to resolving the Incident.

2.8.3 The Service Desk shall monitor Incidents throughout their lifecycle and automatic reminder notifications shall be sent to appropriate resolvers based on Incident Category, Target Initial Response Time and Target Resolution Time.

2.8.4 Subject to clause 2.8.5, the Incident Party that raised an Incident with the Service Desk, an Interested Party, or an Incident Party to which the Incident has been subsequently reassigned by the DCC, may request that the Incident is escalated.

2.8.5 Incidents may be escalated under the following circumstances:

(a) disagreement with categorisation;

(b) Target Initial Response Time has not been met;

(c) Target Resolution Time about to be exceeded;

(d) lack of appropriate response;

(e) dissatisfaction with the progress of an assigned activity;

(f) dissatisfaction with the progress of an Incident; or

(g) dissatisfaction with the resolution of an Incident.

2.8.6 The Service Desk shall include full details of the escalation in the Incident Management Log.

2.9. Escalation Process

2.9.1 Escalated Incidents shall be progressed in accordance with the table below. All escalations shall follow the process and adhere to the sequential order.

Level	DCC		Incident Party
L1 Escalation		Service Desk	Individual nominated to act in the role of service desk operator in accordance with clause 1.4.5
L2 Escalation		Service Desk Manager	Individual nominated to act in the role of service desk manager in accordance with clause 1.4.5
L3 Escalation		Service Manager	Individual nominated to act in the role of Service Manager in accordance with clause 1.4.5
L4 Escalation		Head of Service	Individual nominated to act in the role of Head of Service in accordance with clause 1.4.5
L5 Escalation		Operations Director	Individual nominated to act in the role of Operations Director in accordance with clause 1.4.5

Table 2 – Escalation Process

2.9.2 If, following a Level 5 escalation, a resolution cannot be satisfactorily agreed between the DCC and the escalating organisation, the Incident may be escalated by any Interested Party to the Panel and Section H9.16 shall apply.

2.9.3 The DCC and escalating Incident Party shall provide appropriate evidence to the Panel that it has been through all earlier escalation levels before escalating an Incident to the Panel.

2.10. DCC Major Incidents and Major Security Incidents

2.10.1 All Category 1 Incidents shall also be treated as Major Incidents. Major Security Incidents shall also be treated as Category 1 Incidents.

2.10.2 Once an Incident has been reported to the Service Desk pursuant to clause 2.2.2, the Service Desk shall perform initial triage on the Incident. The Major Incident management process and/or the DCC security team shall be engaged to progress and resolve the Incident where triage confirms that the DCC believes that the Incident should be treated as a Category 1 Incident, unless the circumstances set out in 2.10.7 apply.

2.10.3 If an Incident is updated to become a Category 1 Incident the provisions of this clause 2.10 will also apply.

2.10.4 The DCC shall notify all Incident Parties that are likely to be affected by such Major Incident by a reasonable means in accordance with Section H9.11.

2.10.5 On resolution of the Major Incident, the DCC shall raise a Problem to confirm the Root Cause.

2.10.6 The DCC shall make the details from the Problem available to Interested Parties.

2.10.7 Where a Major Incident has been investigated but then turns out to be an Incident which the DCC is not responsible for resolving (as set out in H9.2(b)) then the Service Desk shall:

(a) Contact the appropriate Incident Party through a Nominated Individual;

(b) assign the Incident to the Incident Party; and

(c) set the Incident status to pending.

2.10.8 Where a Major Incident has been investigated but turns out not to be an Incident:

(a) the Service Desk shall contact the Incident Party that raised the Incident through a Nominated Individual and provide the details to enable the Incident Party to raise and manage the incident within their own system; and

(b) the Service Desk shall set the status of the Incident to closed.

2.10.9 [NOT USED]

Major Security Incidents

2.10.10 Clauses 2.10.11 and 2.10.12 shall apply for a Major Security Incident.

2.10.11 The Incident Party shall notify the Panel, the Security Sub-Committee, in accordance with Section G3, and, pursuant to section H9, the DCC if:

(a) it detects a security Incident within its environment of which the DCC needs to be informed; or

(b) any potential Security Incident it detects appears to relate to the DCC Total System.

2.10.12 The DCC shall notify the Panel and the Security Sub- Committee, in accordance with Section G2, and, pursuant to Section H9, shall inform an Incident Party by an appropriate mechanism if:

(a) any Security Incident occurs that is identified in the Code as requiring notification to the Incident Party or the Panel and Security Subcommittee; or

(b) a Security Incident indicates a breach of the provisions of a Code of Connection.

2.11. Major Incidents not Assigned to the DCC

2.11.1 In the event that a Major Incident is assigned to an Incident Party other than the DCC:

(a) the Incident Party may request that the DCC provides reasonable assistance. When this is requested the DCC shall provide all reasonable assistance to the Incident Party responsible for resolving the Incident in accordance with Section H9.12(b); and

(b) as part of such reasonable assistance, the DCC may disseminate the information to Incident Parties if requested by the Incident Party, using the Self-Service Interface and other mechanisms as appropriate.

2.12. Incident Closure

2.12.1 The rules for the closure of Incidents are detailed below.

2.12.2 An Incident that the DCC is responsible for resolving shall be resolved by the DCC in accordance with the Target Resolution Times set out in the categorisation matrix in clause 2.4.

2.12.3 The Service Desk and the resolver shall each record details of all steps they have each taken to resolve the Incident in the Incident Management Log, as set out in clause 1.4.10.

2.12.4 The Service Desk shall notify the Incident Party and/or other Interested Parties and the resolver via email when the DCC sets the Incident status to resolved.

2.12.5 If the Incident is resolved through the application of a workaround, the Service Desk shall either raise a new Problem or the Incident shall be associated with an existing Problem where one exists.

2.12.6 If it does not consider that the Incident is resolved, the Incident Party, resolver or an Interested Party shall respond to the Service Desk via email or phone call within 3 Working Days, unless a longer period has been agreed by the Service Desk, such agreement to not be unreasonably withheld. In so doing, the relevant party shall provide supporting information as to why they consider the Incident not to be resolved. Then:

(a) If the Service Desk receives, with supporting information, a response detailing that the Incident is not resolved, the Service Desk will change the status from resolved and reassign the Incident for investigation in accordance with Section H9; or

(b) If a response is not received from the Incident Party within the aforementioned timeframe the Service Desk shall close the Incident.

2.12.7 In the event that the Incident Party requires subject matter expert advice before confirming closure and the subject matter expert is unavailable, the Incident Party may contact the Service Desk via email or phone call to request that the closure period be extended.

2.12.8 In the event that the Incident is the result of an intermittent issue the Service Desk shall apply what it reasonably deems to be an appropriate closure period based on the frequency of the occurrences of the issue, and shall close the Incident after this period has elapsed without any further occurrences. The Service Desk shall record this in the Incident Management Log.

2.12.9 After the Incident has been resolved, the Service Desk may raise a Problem and link it to the Incident.

2.13. Re-opening Closed Incidents

2.13.1 The Incident Party that originally raised an Incident may only re-open it if it was closed with a workaround and one of the following circumstances occurs:

(a) the workaround fails; or

(b) the workaround deteriorates to a point that it affects normal business operations.

2.13.2 If a Problem associated with an Incident has been closed, it shall not be possible to re-open the Incident. In this case, the Incident Party shall raise a new Incident.

2.14. Re-occurring Incidents

2.14.1 If a previous Incident reoccurs after it has been closed in line with the procedures in this Incident Management Policy, the Incident Party shall raise a new Incident, in accordance with the provisions set out above.

2.14.2 The DCC may identify re-occurring Incidents by performing trending, correlation and incident matching. Confirmed re-occurrences may be progressed through Problem management.

2.14.3 An Incident Party may identify a re-occurring incident and may notify the DCC. In so doing, the Incident Party shall provide all related Incident reference numbers to the DCC who may progress the issue through Problem management, as set out in clause 3.

3. PROBLEM MANAGEMENT

3.1. Opening a Problem

3.1.1 The DCC shall open a Problem in the Incident Management Log in the following circumstances:

(a) when a Major Incident has been resolved;

(b) when an Incident is closed with a workaround applied; or

(c) when the DCC has identified a re-occurring Incident.

3.1.2 The DCC shall allocate a reasonable initial timescale for carrying out the Root Cause Analysis to enable the re-classification of the Problem as a Known Error.

3.2. Prioritisation and Timescale for Closure of Problems

3.2.1 The DCC shall periodically issue and make available a report listing open Problems to Incident Parties and the Panel.

3.2.2 The report shall set out for each open Problem:

(a) date opened;

(b) Problem classification;

(c) Problem status;

(d) the target closure date;

(e) the anticipated costs (in DCC's reasonable opinion) for the investigation and resolution of the Problem, where appropriate;

(f) the anticipated timescales for the closure of a Problem;

(g) the likely impact on the DCC's business, and its effects on Incident Parties of closing a Problem and continuing with a workaround, highlighting instances where implementing a permanent solution may not be the recommended approach; and

(h) the reason for any target closure date change.

3.2.3 Following the issuing of such a report, the DCC shall discuss with Incident Parties the prioritisation and preferred timescales for the progression of each Problem. Following discussion, and taking respondents' views into account, the DCC shall determine the prioritisation and preferred timescales for the progression of each Problem.

3.2.4 If a Problem investigation or resolution requires a change to the Code a Draft Proposal shall be submitted by the DCC.

3.3. Closing a Problem

3.3.1 The rules for closure of a Problem are detailed below, as required by Section H9.1(k).

3.3.2 Following the application of a permanent fix, the DCC shall discuss the outcome with Interested Parties before closing the Problem.

3.3.3 Details of all steps taken to close the Problem shall be recorded, as set out in Clause 1.4.10.

3.3.4 The DCC shall only close a Problem once one of the following conditions has been met and the DCC has discussed this with Interested Parties that:

(a) the permanent fix has been applied; or

(b) an enhanced and acceptable workaround is in place; or

(c) the DCC will not continue investigations.

3.4. Problem Management for Telefonica UK Limited

3.4.1 The provisions of this Clause 3 shall not apply to matters solely related to Services supported by the SMETS1 SM WAN for which Telefonica UK Limited is the DCC Service Provider.

4. ERROR HANDLING STRATEGY

4.1. The first version of the contents of the Error Handling Strategy will be the 'Error Handling Strategy – DCC Guidance Document' as published by the DCC in June 2016.

4.2. The DCC shall make the Error Handling Strategy available to Users through the Self-Service Interface.

4.3. The DCC may update the Error Handling Strategy from time to time. The DCC shall ensure that Parties are consulted prior to making any changes to the Error Handling Strategy and take into account any relevant views expressed by Parties in making any changes to it.

5. BUSINESS CONTINUITY AND DISASTER RECOVERY

5.1. BCDR General Provisions

5.1.1 Users, Other Parties and Registration Data Providers shall ensure that the contact details provided to the DCC for the purposes of Incident notifications are up to date.

5.1.2 The DCC shall record and treat any Disaster as a Major Incident.

5.1.3 The DCC shall coordinate recovery actions for any Disaster in order to minimise the impact on Services.

5.1.4 The DCC shall notify Incident Parties of a Disaster, with details of the Major Incident and the expected duration of the outage, if any. The DCC shall further inform Incident Parties when Services are restored.

5.1.5 The DCC shall notify Incident Parties of any event that results in a disruption to the Services as set out in Table 4 of this document, with details of the expected duration of the outage, if any. The DCC shall further inform Incident Parties when Services are restored.

5.1.6 The DCC shall implement the processes and arrangements outlined in the tables in clause 5.2 in order to meet the requirements as detailed in Section H10.13.

5.1.7 When requested by the DCC, upon restoration of Services, Incident Parties shall confirm that Services are fully restored.

5.1.8 Upon restoration of Services, if an Incident Party continues to have loss of Services they shall follow the incident management process steps outlined in clause 2.1.

5.2. Business Continuity and Disaster Recovery Procedures

Disaster Recovery

5.2.1 Pursuant to the requirements of Section H10.9:

(a) the DCC shall implement the measures in the table below under 'DCC Mitigation' to reduce the likelihood of the Disaster occurring and limit the impact in the event that a Disaster has occurred;

(b) in the event of a Disaster, the DCC shall follow the actions in the table below detailed under 'DCC Recovery Action'; and

(c) Incident Parties may experience the impact set out in the table below under 'Incident Party Impact' and shall follow the actions as detailed under 'Incident Party Actions on failure, failover or failback'.

Disaster ID	DCC Disaster Impact	DCC Mitigation	DCC Recovery Action	Incident Party Impact	Incident Party Actions on failure, failover or failback	Applicable to SMETS1 or SMETS2+?
D1(a)	The DCC loses the primary data centre provided pursuant to the (data services) contract referred to in paragraph 1.2(a) of Schedule 1 of the DCC Licence.	The DCC shall provide primary and secondary data centres providing data services for the DCC Live Systems, with a resilient server configuration in the primary data centre with an active-passive configuration between data centres. All configurations and data are backed up and backups are stored offsite. There	The DCC shall do one of the following: a. fail over to the secondary data centre; or b. recover Services at the primary data centre.	Incident Parties may experience a loss of all Services on failover to the secondary data centre and on failback to the primary data centre, with the exception of some Testing Services which operate from the secondary data centre.	1. When requested by the DCC, Incident Parties shall suspend submission of Service Requests and Signed Pre-Commands until notified that Services have been restored. 2. Upon restoration of impacted Services, Incident Parties may recommence submission of Service Requests and Signed Pre-Commands (including submitting any that have failed). 3. When requested by the DCC, the Incident Party	SMETS2+

		are resilient network links to the data centres providing communication services.			shall take each of the actions identified in column 6, of rows D5, D8, D9, D10, D11 and D16 of this table 3 and B6, B7 and B12 of table 4 below, as relevant, when DCC fails over from or fails back to the primary data centre.	
D1(b)	The DCC loses the primary data centre provided pursuant to the SMETS1 Data Services contract(s).	The DCC shall provide primary and secondary data centres in order to provide data services for the DCC Live Systems, with a resilient server configuration in the primary data centre with an active-passive configuration between data centres. All configurations and data are backed up and backups are stored offsite. There are resilient network links to the data centres providing communication services.	The DCC shall do one of the following: a. fail over to the secondary data centre; or b. recover Services at the primary data centre.	Incident Parties may experience a partial loss of SMETS1 Services on failover to the secondary data centre and on failback to the primary data centre.	Upon restoration of impacted Services, Incident Parties may recommence submission of SMETS1 Service Requests (including submitting any that have failed).	SMETS1
D2	The DCC loses the secondary data centre provided pursuant to the (data services) contract referred to in paragraph 1.2(a) of Schedule 1 of the DCC Licence.	The DCC shall provide the ability to deliver Testing Services from either the secondary or primary data centres. All configurations & data are backed up & backups are stored offsite. There are resilient network links to the data centres providing communication services.	The DCC shall do one of the following: a. recover Services at the primary data centre; or b. recover Services at the secondary data centre.	Incident Parties will experience a loss of some Testing Services. Incident Parties may experience a loss of some data within Testing Services.	1. When requested by the DCC, Incident Parties shall suspend the use of Testing Services until notified that Services have been restored. 2. Upon Services restoration, Incident Parties may resubmit failed test messages.	SMETS2+
D3(a)	The DCC loses both the primary and secondary data centres provided pursuant to the (data services) contract referred to in paragraph 1.2(a) of Schedule 1 of the DCC Licence.	The DCC shall ensure that all configurations & data are backed up & backups are stored offsite.	The DCC shall do one or more of the following: a. recover Services at the primary data centre; b. recover Services at the secondary data centre; c. restore Services to new infrastructure at an alternative data centre; d. set up network links to the new data centre.	Incident Parties may experience a loss of all Services. Incident Parties may experience a loss of some transactions. Some information related to billing and Service Levels may be lost. On restart the DCC may impose systems-driven Restrictions on transaction volumes/types.	1. When requested by the DCC, Incident Parties shall suspend submission of Service Requests and Signed Pre-Commands until notified that Services have been restored. 2. Upon Services restoration, Incident Parties may resubmit failed messages.	SMETS2+
D3(b)	The DCC loses both the primary and secondary data centres	The DCC shall ensure that all configurations & data are backed up	The DCC shall do one or more of the following: a. recover Services at the primary	Incident Parties may experience a partial loss of all SMETS1 Services. Incident Parties may	Upon restoration of impacted Services, Incident Parties shall resubmit any that have failed SMETS1 Service Requests.	SMETS1

	provided pursuant to the SMETS1 Data Services.	& backups are stored offsite.	data centre; b. recover Services at the secondary data centre; c. restore Services to new infrastructure at an alternative data centre; d. set up network links to the new data centre.	experience a loss of some SMETS1 transactions to a particular S1SP. On restart the DCC may impose systems-driven Restrictions on transaction volumes/types.		
D4	DCC Services are impacted by a virus or malware	The DCC constantly monitors its environments and networks to ensure the integrity of firewalls and anti-virus measures.	The DCC shall do one or more of the following: a. halt processing and clear the virus or malware; b. failover to a secondary data centre (or primary data centre) in the case of Testing Services; c. isolate the affected system and clear the virus or malware; d. cease to process transactions from Incident Parties impacted by the virus or malware until confirmation is received that they have applied necessary measures; e. apply any software patches to its Services; or f. recover from backup.	Incident Parties may experience a loss or interruption to affected Services. The DCC may impose systems-driven restrictions on transaction volumes/types on restart. Additional impacts are detailed in column 5 of rows D2, D5 to D12 and D15 of this table.	1. When requested by the DCC, Incident Parties shall suspend use of any affected Services. 2. Prior to re-commencement of Service provision, the DCC may request that each Incident Party confirms that it has cleaned its User Systems and applied necessary measures to prevent the virus or malware reoccurring. 3. When requested by the DCC, the Incident Party shall take each of the actions identified in column 6, of rows D5, D8, D9, D10, D11 and D16 of this table 3 and B6, B7 and B12 of table 4 below, as relevant, when DCC fails over from or fails back to the primary data centre.	SMETS1 and SMETS2+
D5	The DCC's experiences a failure of the part of the DCC Systems responsible for delivering Service Requests, Commands, Responses & Alerts	The DCC shall provide primary & secondary data centres providing data services for the DCC Live Systems, with resilient server configuration in the primary data centre with an active-passive configuration between data centres. All configurations & data are backed up & backups are stored offsite. There are resilient network links to the data centres providing communication services.	The DCC shall do one of the following: a. fail over to the secondary data centre; or b. recover Services at the primary data centre.	Incident Parties may experience a loss of Communication, Enrolment and Local Command Services. Incident Parties may experience a loss of all Services, with the exception of some Testing services which operate from the secondary data centre, during failover to the secondary data centre and failback to the primary data centre.	1. When requested by the DCC, Incident Parties shall suspend until notified that Services have been restored: • in respect of SMETS2+, the submission of Service Requests and Signed Pre-Commands; and • in respect of SMETS1, the submission of SMETS1 Service Requests. 2. Upon restoration of impacted Services, Incident Parties may recommence submission (including submitting any that have failed) of: • in respect of SMETS2+, Service Requests and	SMETS1 and SMETS2+

					Signed Pre-Commands; and • in respect of SMETS1, SMETS1 Service Requests. 3. When requested by the DCC, the Incident Party shall take each of the actions identified in column 6, of rows D8, D9, D10, D11 and D16 of this table 3 and B6, B7 and B12 of table 4 below, as relevant, when DCC fails over from or fails back to the primary data centre.	
D6	Intentionally Blank					
D7	Intentionally Blank					
D8	The DCC experiences a failure of the systems used to support the operation of the CoS Party.	The DCC shall provide primary & secondary data centres providing data services for the DCC Live Systems, with resilient server configuration in the primary data centre with an active-passive configuration between data centres. All configurations & data are backed up & backups are stored offsite. There are resilient network links to the data centres providing communication services.	The DCC shall do one of the following: a. fail over to the secondary data centre; or b. recover Services at the primary data centre.	Incident Parties would be unable to successfully send CoS Update Security Credentials Service Requests. Incident Parties may experience a loss of all Services during the failover to the secondary data centre. Incident Parties would also experience a loss of all Services on failback to the primary data centre.	1. When requested by the DCC, Incident Parties shall suspend until notified that Services have been restored: • in respect of SMETS2+, the submission of Service Requests and Signed Pre-Commands; and • in respect of SMETS1, the submission of SMETS1 Service Requests. 2. Upon restoration of impacted Services, Incident Parties may recommence submission (including submitting any that have failed) of: • in respect of SMETS2+, Service Requests and Signed Pre-Commands; and • in respect of SMETS1, SMETS1 Service Requests. 3. When requested by the DCC, the Incident Party shall take each of the actions identified in column 6, of rows D5, D9, D10, D11 and D16 of this table 3 and B6, B7 and B12 of table 4 below, as relevant, when DCC fails over from or fails back to the primary data centre.	SMETS1 and SMETS2+
D9	The DCC experiences a loss of connectivity to one or more Incident Parties	The DCC shall provide primary & secondary data centres providing data services for the DCC Live Systems, with resilient server	The DCC shall do one or more of the following: a. recover connection at the primary data centre; b. recover	Incident Parties will experience loss of connectivity to Services via the DCC User Gateway Connection.	1. In the event of a Services interruption, when advised by the DCC, Incident Parties shall suspend submission via the DCC User Gateway Connection until Services are restored	SMETS1 and SMETS2+

		configuration in the primary data centre with an active-passive configuration between data centres. There are resilient network links to the DCC User Gateway Connection with automatic rerouting between both data centres.	connection at the secondary data centre; c. recover User connection.		of: • In respect of SMETS2+, Service Requests and Signed Pre-Commands; and • in respect of SMETS1, SMETS1 Service Requests. 2. In the event of a Services interruption, when requested by the DCC, Incident Parties shall only submit Category 1 Incidents. 3. Upon restoration of impacted Services, Incident Parties may recommence submission (including submitting any that have failed) of: • In respect of SMETS2+, Service Requests and Signed Pre-Commands; and • in respect of SMETS1, SMETS1 Service Requests.	
D10	The DCC experiences a failure of the systems used to support the Self-Service Interface	The DCC shall provide primary & secondary data centres providing data services for the DCC Live Systems, with resilient server configuration in the primary data centre with an active-passive configuration between data centres. All configurations & data shall be backed up & backups are stored offsite. There are resilient network links to the DCC User Gateway Connection with automatic rerouting between both data centres.	The DCC shall do one of the following: a. fail over to the secondary data centre; or b. recover Services at the primary data centre.	Incident Parties would experience loss of connectivity to Services via the Self-Service Interface. Incident Parties may experience a loss of all Services, with the exception of some Testing services which operate from the secondary data centre during the failover to the secondary data centre and on failback to the primary data centre.	1. When requested by the DCC, Incident Parties shall suspend until notified that Services have been restored submission of: • In respect of SMETS2+, Service Requests and Signed Pre-Commands; and • in respect of SMETS1, SMETS1 Service Requests. 2. Upon restoration of impacted Services, Incident Parties may recommence submission of Service Requests and Signed Pre-Commands (including submitting any that have failed). 3. Incident Parties may need to log in to the Self-Service Interface again. 4. When requested by the DCC, the Incident Party shall take each of the actions identified in column 6, of rows D5, D8, D9, D11 and D16 of this table 3 and B6, B7 and B12 of table 4 below, as relevant, when DCC fails over from or fails back to the primary data centre.	SMETS1 and SMETS2+
D11(a)	The DCC experiences a failure of the connection between the service providers	The DCC shall provide primary & secondary data centres providing data services for the DCC Live Systems,	The DCC shall do one of the following: a. fail over to the secondary data centre; or b. recover	Incident Parties may experience a delay or failure in the processing of Service Requests, Commands, Responses and Alerts.	1. When requested by the DCC, Incident Parties shall suspend submission of Service Requests and Signed Pre-Commands until notified that Services	SMETS2+

	referred to in paragraphs 1.2(a) and 1.2(b) of Schedule 1 of the DCC Licence (DCC WAN Gateway).	with resilient server configuration in the primary data centre with an active-passive configuration between data centres. All configurations & data shall be backed up & backups are stored offsite. There are resilient network links to the data centres providing communication services. Commands, Responses & Alerts shall be cached.	connection at the primary data centre.	Incident Parties may experience a loss of all Services during the failover to the secondary data centre. Incident Parties would also experience a short impact on all Services on failback to the primary data centre.	have been restored. 2. Upon restoration of impacted Services, Incident Parties may recommence submission of Service Requests and Signed Pre-Commands (including submitting any that have failed). 3. When requested by the DCC, the Incident Party shall take each of the actions identified in column 6, of rows D5, D8, D9, D10 and D16 of this table 3 and B6, B7 and B12 of table 4 below, as relevant, when DCC fails over from or fails back to the primary data centre.	
D11(b)	The DCC experiences a failure of the connection between the DSP and the SMETS1 Data Service Providers (SMETS1 Management Gateway).	The DCC shall provide primary & secondary data centres providing data services for the DCC Live Systems, with resilient server configuration in the primary data centre with an active-passive configuration between data centres. All configurations & data shall be backed up & backups are stored offsite. There are resilient network links to the data centres providing communication services. Commands, Responses & Alerts shall be cached.	The DCC shall do one of the following: a. fail over to the secondary data centre; or b. recover connection at the primary data centre.	Incident Parties may experience a delay or failure in the processing of Service Requests, Commands, Responses and Alerts. Incident Parties may experience a loss of all Services during the failover to the secondary data centre.	Upon restoration of impacted Services, Incident Parties may recommence submission of SMETS1 Service Requests (including submitting any that have failed).	SMETS1
D12	Intentionally Blank					
D13	The DCC loses its primary data centre provided pursuant to the (SMKI) contract referred to in Schedule 1 of the DCC Licence.	The DCC shall provide instances of the SMKI service infrastructure at primary & secondary SMKI data centres in an active-passive configuration with full data replication between sites and resilient network links to the Data Service Provider. The DCC shall backup all SMKI configurations & data and shall store backups offsite.	The DCC shall do one of the following: a. fail over to the secondary data centre; or b. recover Services at the primary data centre.	Incident Parties would be unable to request new Organisational or Device Certificates during failure, failover or failback to the primary data centre.	1. When requested by the DCC, Incident Parties shall suspend transmission of Certificate Signing Requests. 2. Upon restoration of impacted Services, Incident Parties may recommence submission of Certificate Signing Requests (including submitting any that have failed).	SMETS1 and SMETS2+
D14	The DCC loses both primary & secondary data	The DCC shall maintain full off-site	The DCC shall: a. Restore failed services at one of	Incident Parties may be unable to request new	1. When requested by the DCC, Incident Parties shall suspend submission of	SMETS1 2 and SMETS2+

	centres provided pursuant to the (SMKI) contract referred to in Schedule 1 of the DCC Licence.	configuration & data backups.	the existing datacentres; or b. restore failed Services to new infrastructure at an alternative data centre and shall then redirect network links to the alternate data centre.	Organisational or Device Certificates.	Certificate Signing Requests until Services have been restored. 2. Upon Services restoration, Incident Parties may resubmit failed Certificate Signing Requests.	
D15(a)	The DCC loses both primary data centres provided pursuant to the DCO (Dual Control Organisation) contract.	The DCC shall provide primary and secondary data centres in order to provide data services for the DCC Live Systems, with a resilient server configuration in the primary data centre with an active-passive configuration between data centres. All configurations and data are backed up and backups are stored offsite. There are resilient network links to the data centres providing communication services.	The DCC shall do one of the following: a. fail over to the secondary data centre; or b. recover Services at the primary data centre.	Incident Parties may experience a partial loss of SMETS1 Services on failover to the secondary data centre and on failback to the primary data centre.	Upon restoration of impacted Services, Incident Parties may recommence submission of SMETS1 Service Requests (including submitting any that have failed).	SMETS1
D15 (b)	The DCC loses both primary & secondary data centres provided pursuant to the (Dual Control Organisation) contract.	The DCC shall maintain full off-site configuration & data backups.	The DCC shall do one or more of the following: a. recover Services at the primary data centre; b. recover Services at the secondary data centre; c. restore Services to new infrastructure at an alternative data centre; or d. set up network links to the new data centre.	Incident Parties will experience a loss of all SMETS1 Services. Incident Parties may experience a loss of some SMETS1 transactions to a particular S1SP. On restart the DCC may impose systems-driven Restrictions on transaction volumes/types.	1. When requested by the DCC, Incident Parties shall suspend submission of all SMETS 1 Service Requests until Services have been restored. 2. Upon restoration of impacted Services, Incident Parties may recommence submission of SMETS1 Service Requests (including submitting any that have failed).	SMETS1
D16	A failure of a connection or interface between one or more Registration Data Providers (RDP) and the DCC	There are resilient network links to the Registration Data Providers from both primary and secondary data centres.	The DCC shall do one or more of the following: a. recover connection at the primary data centre; b. recover connection at the secondary data centre; c. recover connection to the Registration Data Provider; or d. Send Registration update by	There may be a delay in the issuing of DCC Status Files.	1. Upon service restoration, Incident Parties may resubmit failed Service Requests and/or SMETS1 Service Requests. 2. When requested by the DCC, RDPs shall receive updates by alternative (secure) means.	SMETS1 and SMETS2+

			alternative (secure) means.			
D17	The DCC loses a data centre provided pursuant to the (communications services) contract referred to in paragraph 1.2(b) of Schedule 1 of the DCC Licence.	The DCC shall provide primary & secondary sites for communication services data centres in an active-active configuration. All configurations & data are backed up and backups are stored offsite. In the event of failure of one communications service data centre, Services would continue to be provided from the secondary data centre.	The DCC shall: a. restore the provision of Impacted Services at the affected communications data centre; or b. restore the provision of impacted Services at a new data centre.	There would be no impact on Incident Parties from a single communications service data centre failure. Restoration of the existing data centre will not impact Incident Parties.	1. No action would be required from Incident Parties to resolve this Incident. 2. Restoration of the existing data centre will not require action from Incident Parties.	SMETS1 and SMETS2+
D18	The DCC loses both data centres provided pursuant to the (communications services) contract referred to in paragraph 1.2(b) of Schedule 1 of the DCC Licence.	The DCC shall maintain full off-site configuration & data backups.	The DCC shall: a. restore impacted Services to new infrastructure at the affected location(s); or b. restore services at an alternative data centre(s)	Incident Parties may be unable to send Commands to Devices or receive Responses and Device Alerts via the DCC and will experience loss of some Services.	1. When requested by the DCC, Incident Parties shall suspend submission until notified that Services have been restored of: • In respect of SMETS2+, Service Requests and Signed Pre-Commands; and • in respect of SMETS1, SMETS1 Service Requests. 2. Incident Parties shall also comply with all reasonable DCC requests to assist with prioritising & phasing back transmission of Service Requests and/or SMETS1 Service Requests.	SMETS1 and SMETS2+
D19	The service provided pursuant to the contract referred to in paragraph 1.2(b) of Schedule 1 of the DCC Licence experiences multiple access node failure (Failure of a single access node would not be regarded as a DCC Disaster).	The DCC has significant, although not complete, overlap between access nodes. The DCC shall ensure that access nodes are of a resilient design and that it has sufficient provision of mobile equipment and components spares to restore service within acceptable timescales.	The DCC shall: deploy field maintenance and/or mobile equipment to restore Services.	Incident Parties may experience the failure of impacted Services directed to meters, Communications Hubs and Gas Proxy Functions in the affected area(s).	Upon Services restoration, Incident Parties may resubmit failed Service Requests and/or SMETS1 Service Requests.	SMETS1 and SMETS2+
D20	Communications Hub Product Recall	The DCC has more than one source for Communications Hubs. Buffer stocks are held by the DCC and Communications Hub manufacturers.	The DCC shall: a. determine the nature and extent of the problem; and b. notify all Incident Parties of the extent of product recall required and effects on existing stocks	This could result in Incident Parties diverting field staff to uninstall affected Communications Hubs, resulting in delays in installations. It might also impact stocks and future supply.	Incident Parties shall provide reasonable assistance to the DCC in resolving issues.	SMETS2+

			and future supply.			
D21	Loss of a site housing a DCC service function	The DCC shall have arrangements in place to resume all activity at an alternate location as part of its business continuity arrangements.	The DCC shall: a. relocate the service function to the designated recovery site & shall restore service from there; or b. recover services at existing site	Incident Parties may be unable to contact the affected service function until it has been recovered at an alternate location.	There is no action required from Incident Parties.	SMETS1 and SMETS2+
D22	Intentionally Blank					

Table 3 – Disaster Recovery Procedures

Business Continuity

5.2.2 Pursuant to the requirements of Section H10.9:

(a) the DCC shall implement the measures in the table below under 'DCC Mitigation' to reduce the likelihood of a Business Continuity Event occurring and limit the impact in the event that a Business Continuity Event has occurred;

(b) in the event of the occurrence of a Business Continuity Event, the DCC shall follow the actions in the table below detailed under 'DCC Recovery Action'; and

(c) Incident Parties may experience the impact set out in the table below under 'Incident Party Impact' and shall follow the actions as detailed under 'Incident Party Actions on failure, failover or failback'.

Business Continuity ID	**DCC BC Impact**	**DCC Mitigation**	**DCC Recovery Action**	**Incident Party Impact**	**Incident Party Actions on failure, failover or failback**
B6	The DCC experiences a failure of the systems used to support the provision of service management.	The DCC shall provide primary & secondary data centres providing data services for the DCC Live Systems, with resilient server configuration in the primary data centre with an active-passive configuration between data centres. All configurations & data are backed up & backups are stored offsite. There are resilient network links to the data centres providing communication services.	The DCC shall do one of the following: 1. fail over to the secondary data centre; or 2. recover Services at the primary data centre; and 3. the DCC Service Desk shall capture Incidents using another method until it regains access to the Service Management System.	Incident Parties may be unable to raise incidents or access incident information via the Self-Service Interface. Incident Parties may experience a loss of all Services, with the exception of some Testing services which operate from the secondary data centre during the failover to the secondary data centre and on failback to the primary data centre.	1. When requested by DCC, Incident Parties may only submit Category 1 Incidents. 2. Upon Services restoration, Incident Parties may submit outstanding Incidents. 3. When requested by the DCC, the Incident Party shall take each of the actions identified in column 6, of rows D5, D8, D9, D10, D11 and D15 of table 3 above and B6, B7 and B12 of this table 4, as relevant, when DCC fails over from or fails back to the primary data centre.
B7	The DCC experiences a failure of the systems used to support the provision	The DCC shall provide primary & secondary data centres providing data services for the DCC Live Systems, with resilient	The DCC shall do one of the following: 1. fail over to the secondary data	Incident Parties may experience unavailability of preconfigured reports via the	1. When requested by the DCC, Incident Parties shall suspend submission of Service

	of data warehousing and reporting.	server configuration in the primary data centre with an active-passive configuration between data centres. All configurations & data are backed up & backups are stored offsite. There are resilient network links to the data centres providing communication services.	centre; or 2. recover Services at the primary data centre.	Self-Service Interface. Incident Parties may experience a loss of all Services, with the exception of some Testing services which operate from the secondary data centre during the failover to the secondary data centre and on failback to the primary data centre.	Requests and Signed Pre-Commands until notified that Services have been restored. 2. Upon restoration of impacted Services, Incident Parties may recommence submission of Service Requests and Signed Pre-Commands (including submitting any that have failed). 3. When requested by the DCC, the Incident Party shall take each of the actions identified in column 6, of rows D5, D8, D9, D10, D11 and D15 of table 3 above and B6, B7 and B12 of this table 4, as relevant, when DCC fails over from or fails back to the primary data centre.
B12	Loss of the systems used to support Communications Hub ordering.	The DCC shall provide dual instances of the order management system in resilient configuration across primary and secondary data centres. All configurations & data are backed up with backups stored offsite. The DCC shall provide multiple network links & diverse routing.	The DCC shall do one or more of the following: 1. Capture orders using electronic or paper forms; 2. Restore the system from backups; and 3. On restoration of the system, the DCC shall ensure that all captured orders are entered.	Restoration of the CH Ordering System will not impact Incident Parties.	1. In the event of a service interruption, Incident Parties shall submit orders as requested by the DCC. 2. No action is required from Incident Parties on restoration of the system.

Table 4 – Business Continuity Procedures

6. Business Continuity and Disaster Recovery for Vodafone Global Enterprise Limited and Telefonica UK Limited

6.1. The provisions of Section H10.13 shall not apply to the Services supported by the SMETS1 SM WAN for which Vodafone Global Enterprise Limited or Telefonica UK Limited is the DCC Service Provider.

6.2. On the occurrence of a Disaster affecting the SMETS1 SM WAN for which either Vodafone Global Enterprise Limited or Telefonica UK Limited is the DCC Service Provider, the DCC shall take reasonable steps to restore any and all affected Services.

6.3. The requirements of Section H10.11 shall not apply to the Services supported by the SMETS1 SM WAN for which Telefonica UK Limited is the DCC Service Provider.

7. Planned Maintenance for Vodafone Global Enterprise Limited and Telefonica UK Limited

7.1. The requirements of Section H8.4 shall not apply to Planned Maintenance of the SMETS1 SM WAN for which Vodafone Global Enterprise Limited is the DCC Service Provider. The requirements of Sections H8.3

and H8.4 shall not apply to Planned Maintenance of the SMETS1 SM WAN for which Telefonica UK Limited is the DCC Service Provider.

7.2. Where Planned Maintenance is proposed to the SMETS1 SM WAN for which Vodafone Global Enterprise Limited or Telefonica UK Limited is the DCC Service Provider, the DCC will take reasonable steps to provide notice to Parties, to Registration Data Providers and to the Technical Architecture and Business Architecture Sub-Committee of the Planned Maintenance setting out the following information:

(a) the proposed Maintenance activity (in reasonable detail);

(b) the parts of the Services that will be disrupted (or in respect of which there is a Material Risk of disruption) during each such Maintenance activity;

(c) the time and duration of the Maintenance activity; and

(d) any associated risk that may subsequently affect the return of normal Services.

DCC shall take reasonable steps to provide such notice at least 4 (four) Working Days in advance where Vodafone Global Enterprise Limited is the DCC Service Provider and at least 6 (six) Working Days in advance where Telefonica UK Limited is the DCC Service Provider.

Version AH 2.0

Appendix AH

Self-Service Interface Access Control Specification

Definitions

In this document, except where the context otherwise requires:

- expressions defined in Section A1 of the Code (Definitions) have the same meaning as is set out in that Section;
- the expressions in the left-hand column below shall have the meanings given to them in the right-hand column below; and
- any expressions not defined here or in Section A1 of the Code have the meaning given to them either in the DCC User Interface Specification or the Self-Service Interface Code of Connection.

Business Functional Domain	means a grouping of one or more Functional Components which is used to describe and deliver the functional requirements of Self-Service Interface Users.
Functional Component	means a specific item or set of functionality provided by the Self-Service Interface which is subject to the access controls set out in this Appendix AH.
Job Type Role	means one of the functional roles as set out in the table contained in clause 1.5.2
Order Management System (OMS)	as defined in the CH Handover Support Materials
Security Assertion Markup Language (SAML)	an open, published framework for exchanging security information between online business partners
SSI Baseline Requirements Document	means a document which sets out the design specification of the Self-Service Interface, and which is maintained by the DCC in accordance with Section 1 of this Appendix AH.

1. SELF-SERVICE INTERFACE ACCESS CONTROL SPECIFICATION

The DCC shall ensure that, where the DCC receives a request to access the Self-Service Interface, it shall direct that request to the appropriate URL for dealing with that request, and that such URL shall be implemented and maintained such that communications across it can be authenticated.

Where any fields are found to be invalid, the DCC shall ensure that validation error messages and suggestions for resolution are provided.

1.1. Authorisation

The DCC shall ensure that each user of the Self-Service Interface shall only be permitted to access a Functional Component if it is entitled to do so pursuant to clause 1.5.1 and 1.5.2 given the User ID(s) and Job Type Role(s) that are supplied as attributes of the SAML assertion.

1.2. SAML Authentication

The DCC shall provide to Users a SAML-capable Identity Provider Service for the purpose of authentication of User Personnel to the Self-Service Interface (the "DCC Identity Provider Service").

Each User may use an Identity Provider Service that is not the DCC Identity Provider Service for the purpose of authentication of its User Personnel to the Self- Service Interface.

To authenticate each request from a User Personnel that seeks to access the Self-Service Interface, the DCC shall use either:

(a). a SAML assertion provided by the DCC Identity Provider Service (as defined in clause 1.3); or

(b). a SAML assertion provided by an Identity Provider Service provided by the User (as defined in clause 1.4).

After an Identity Provider Service provides the User Personnel's SAML assertion, the DCC shall store a secure cookie in the User Personnel's browser. Such secure cookie shall be set to expire 8.5 hours after initial authentication by:

(a) the DCC, for the DCC Identity Provider Service; or

(b) the User, where such User is using an Identity Provider Service that is not the DCC Identity Provider Service.

If this cookie exists during subsequent authentication, the DCC shall bypass SAML authentication. Where using either the DCC Identity Provider Service or any other Identity Provider Service, if a User wishes to change the rights of that User Personnel to access the Self-Service Interface, the User shall delete the cookie from the User Personnel's browser cookie store.

The User shall ensure that its browser uses HTTP POST to transfer SAML between its Identity Provider Service and the Self-Service Interface.

Each User shall ensure that SAML assertions are applied when requesting access to the Self-Service Interface.

Each User must, when using any Identity Provider Service, present the Job Type Role(s) for which access to the Functional Component is being requested in the SAML assertion sent to the DCC.

Each User shall ensure that each SAML assertion includes a Digital Signature produced by a DCCKI Digital Signing Key associated with a DCCKI Infrastructure Certificate in accordance with the FIPS 186-4 Digital Signature Standard using SHA-256 hashing algorithm. The User shall ensure that a SHA-256 hashing algorithm is applied to the SAML assertion.

1.3. SAML Authentication via the DCC Identity Provider Service

Where a User Personnel attempts to access the Self-Service Interface and a non-expired cookie is not stored in the User Personnel's browser cookie store:

1. The DCC shall send a SAML assertion request to the DCC Identity Provider Service via the User Personnel's browser;

2. When requested, the User shall provide the requested credentials (username, password, and certificate) to the DCC Identity Provider Service;

3. As set out in clause 1.1, the DCC shall grant or deny that person's access to the Self-Service Interface by providing a cookie enabling such access to be stored in the User Personnel's browser cookie store. If access is denied, the DCC shall provide a browser message which requests that the User Personnel resubmits their credentials.

The DCC shall ensure that, where a User is using the DCC Identity Provider Service, access to the Self-Service Interface is only provided once a User Personnel performs a login and generates a new password the first time that it uses that Identity Provider Service.

1.4. SAML Authentication via an Identity Provider Service that is not the DCC Identity Provider Service

When using an Identity Provider Service that is not the DCC Identity Provider Service, the User shall comply with this clause 1.4.

1.4.1 Authentication Requirements

A User providing a SAML assertion when seeking to access the Self-Service Interface via an Identity Provider Service that is not the DCC Identity Provider Service, shall ensure that its Identity Provider Service:

- prompts the User Personnel to provide their credentials (username, password, and certificate); and

- validates the User Personnel's credentials and (only where successfully validated) sends a SAML response including a SAML assertion to the Self-Service Interface.

The User shall ensure that SAML assertions, provided to the DCC by its Identity Provider Service, comply with the OASIS Standard – Assertions and Protocols for the OASIS Security Assertion Markup Language (SAML) v2.0.

The User shall ensure that the Identity Provider Service authentication mechanism shall use an appropriate SAML security assertion to demonstrate conformance to UK Government Authentication Framework Level 2.

1.4.2 Enrolment of an Identity Provider Service that is not the DCC Identity Provider Service

Where using an Identify Provider Service that is not the DCC Identify Provider Service, prior to seeking to access the Self-Service Interface for the first time, the User shall obtain at least one DCCKI Infrastructure Certificate in accordance with the DCCKI RAPP, and shall install such DCCKI Certificates on its Identity Provider Service.

The User shall configure their Identity Provider Service as defined in clause 1.4.1 and export and send a copy of the Identity Provider Service metadata to the DCC via secured electronic means, where such metadata shall include the URL of the Identify Provider Service and contact details in respect of the Identity Provider Service. Where the DCC reasonably requires the metadata to include additional information, the DCC shall inform the User of the information required and the User shall provide the information requested.

1.4.3 SAML Profiles, Bindings and Protocols

The User shall ensure that the Identity Provider Service it uses supports the following SAML profile, binding and protocol:

Profile	Web Browser SSO (single sign-on)
Binding	HTTP POST (HTTP/1.1)
Protocol	Authentication Request Protocol

1.4.4 Identity Provider Service SAML Configuration

Where a User notifies the DCC that it wishes to use an Identity Provider Service that is not the DCC Identity Provider Service, the DCC shall upon request provide, to that User via secured electronic means, the following information to be included in each SAML assertion:

- the service provider unique ID to be used by the Identity Provider Service, which is denoted as '[UNIQUE IDENTIFIER SP]' in the SAML attributes list below; and
- the URL formatted identifier of the Self-Service Interface, which is denoted as '[DCC SP URL]' in the SAML attributes list below.

The User shall ensure that their Identity Provider Service:

- shall not sign Authentication Requests (AuthnRequest);
- shall sign SAML Assertions;
- shall not sign Authentication responses;
- shall not encrypt any part of the SAML assertion (other than the Digital Signature);
- shall use persistent and unique nameIDs;
- shall only include NotBefore, NotOnOrAfter or AudienceRestriction in the SAML Condition elements; and
- shall set the SAML assertion nameID to be persistent and unique to the User Personnel.

The User shall ensure that their Identity Provider Service sets the following SAML attributes shown in square brackets, making reference to the information shown after each colon:

- [UNIQUE IDENTIFIER IDP]: a unique ID assigned to the SAML response by the Identity Provider Service.
- [UNIQUE IDENTIFIER SP]: the service provider unique ID for the SAML request, as provided by the DCC.
- [TIMESTAMP]: a timestamp in standard SAML format.
- [DCC SP URL]: the URL formatted identifier for the Self-Service Interface, as provided by the DCC.
- [IDP ISSUER URL]: a URL identifying the Identity Provider Service issuing the SAML assertion.
- [SAML ASSERTION UNIQUE IDENTIFIER]: a unique identifier assigned to the SAML assertion by the Identity Provider Service.

- [MESSAGE SIGNATURE]: a Digital Signature generated by the signing of the SAML assertion message using the DCCKI Digital Signing Key associated with a DCCKI Infrastructure Certificate.

- [USERNAME]: a unique username assigned to the User Personnel by the Identity Provider Service.

- [SESSION EXPIRY]: a valid SAML date/time object describing the expiry time of the session associated with the user.

- [ASSERTION START]: a valid SAML date/time object describing the start time of the validity of the SAML assertion.

- [ASSERTION EXPIRY]: a valid SAML date/time object describing the expiry time of the validity of the SAML assertion.

- [SAML AUTHENTICATION CONTEXT]: a valid SAML Authentication Context Class describing the authentication that the user has completed with the Identity Provider Service.

- [Role name]: Job Type Role(s) as described in section 1.5. Multiple roles should be specified by separating role names using commas (,).

- [OrgID]: a list of User ID(s) in relation to which the User has been granted permission to access information held on the Self-Service Interface by the other User(s) to whom that information pertains. Such permission having been granted in accordance with clause 1.1.1 and not having been rescinded in accordance with clause 1.5.4. Multiple User IDs should be specified by separating values with commas (,).

1.5. Roles

1.5.1 DCC defined access

The DCC shall provide to User Personnel of each User access to each Functional Component that the User is eligible to access as set out in Section H8.16 or, where not specified in Section H8.16, as set out in this clause 1.5. Such access shall either be full or conditional, where:

- 'Full' means that the User can access data and use all functions associated with the specific Functional Component; and

- 'Conditional' means that a User’s entitlement to access data and use all functions associated with the specific Functional Component is based on the access rules for conditional access set out below.

BFD ID	Business Functional Domain Name	Service capability	Functional Component	DCC Defined Access
			Raise service management Incidents UC_RaiseSMI_001 UC_RaiseSMI_002	Full

BFD01	Service Management	Provide service management capabilities in accordance with H9.4 and the Incident Management Policy, enabling Users to: • Raise, update, view and track Incidents. • Track and view detailed Problem information related to Incidents.	UC_RaiseSMI_003 UC_RaiseSMI_004	
			Update service management Incidents UC_UpdateSMI_001	Conditional. Access shall be granted as set out in Section H9.
			View service management Incidents UC_ViewSMI_001 UC_ViewSMI_002	Conditional. Access shall be granted as set out in Section H9.
			Problem management UC_ProblemManagement_001, UC_ProblemManagement_002	Conditional. Access shall be granted in accordance with Section H9.
BFD02	Smart Metering Inventory	Enable Users to search and query current information on Smart Meter Inventory down to individual Devices in accordance with H8.16(a). Provide detailed information on a Device and any associated Devices.	Smart metering inventory UC_Inventory_001, UC_Inventory_002	Full
BFD03	DCC Service Status	Provide Users with a dashboard of component availability for DCC Services in accordance with H8.16(g).	DCC service status UC_ServiceDashboard_001	Full
BFD04	Service Audit Trails	Enable Users to query information on Service Audit Trails, showing a record of service activity in accordance with H8.16(b). Only the records pertaining to that User will be shown in search and individual message view, where the records pertaining to a User are those for: • the User IDs for that User; and • any User IDs for which that User has been granted permission to access the information in accordance with clause 2.5.3 and such permission has not been rescinded in accordance with clause 2.5.4.	Service Audit Trails UC_ServiceAudit_001, UC_ServiceAudit_002	Conditional. Access shall be granted as set out in Section H8.16(b).
BFD05	Forward Schedule of Change	Enable Users to query and view detailed information on Planned Maintenance, changes scheduled or change freezes affecting any of the following elements of	Forward schedule of change UC_Schedule_001,	Full

		DCC Smart Metering ecosystem in accordance with H8.16(g): • Communications Hub firmware. • Parse & Correlate software. • SMIKI software. • DCC-impacting SEC Releases. • Other major DCC releases. • Meter firmware (Meter firmware events will only be visible to Users for Devices for which they are the Responsible Supplier)	UC_Schedule_002, UC_Schedule_003	
BFD06	Meter Read Transactions	Enable Users to query information on Meter Read Transactions for all users in accordance with H8.16(c).	Meter Read Transactions UC_Inventory_001	Full
BFD07	CSP SMWAN Network Coverage	Enable Users to query information on SM WAN network coverage down to premises level across each of the three GB regions in accordance with H8.16(f).	SM WAN network coverage UC_CSPCoverage_001 UC_CSPCoverage_002	Full
BFD08	DCC Service Alerts	Enable Users to view details of any Service affecting news / Alerts and other useful text relating to the quality of service delivery and service management in accordance with H8.16(g).	DCC Service Alerts UC_ServiceAlerts_001, UC_ServiceAlerts_002	Full
BFD09	Service Requests	Enable Users to: • Browse a catalogue of available DCC Service Requests. • Raise and update service management Service Requests with DCC from their service catalogue. Enables Users to track and update the status of raised requests within DCC service management system. • View full details of the raised Service Request User Personnel will only be able to access requests raised by the User with which they are associated.	Service catalogue publication and call off UC_ServiceCatalogue_001, UC_ServiceCatalogue_002, UC_ServiceCatalogue_003	Full
BFD10	Communications Hub Availability & Diagnostics	Enable Users to query information on Communication Hub availability and diagnostics down to individual Communications Hubs. Allows Users to attempt to diagnose and resolve Incidents	Communications Hub availability and diagnostics UC_HubStatus_001 UC_HubStatus_002	Conditional. Access shall be granted to the Responsible Supplier, the

		relating to any Communications Hubs for which they are the Responsible Supplier, the Network Party or Registered Supplier Agent, using DCC's remote diagnostic tools.		Network Party or Registered Supplier Agent for any Smart Metering System of which the Communications Hub Function in question forms a part.

BFD11	Reporting	Enable users to access on demand a standard set of pre-defined reports. Allow Users to view and download individual reports from a defined set of published reports.	Reporting UC_Reports_001	Conditional. Users will only be permitted to view reports which pertain to them.

BFD12	Knowledge Management, Search and FAQ's	Enable Users to access the following functionality in accordance with H8.16(g) where applicable: • Knowledge management. This allows Users to view help and support information enabling early triage of User issues and queries, including access to the anonymous resolution details of service management problems and Incidents. • FAQ information. • DCC User Manuals detailing the operation of DCC Services. • Search capability, allowing Users to search for content provided by the SSI using tagged keywords, or textual content of page titles and descriptions.	Knowledge management UC_KnowledgeManagement_001	Full
			FAQs UC_FAQ_001	Full
			DCC user manuals UC_Manuals_001	Full
			UC_Search_001	Full

BFD13	Forecasting and Ordering	Enable Users to access OMS in accordance with H8.16(e). In OMS Users can submit orders and forecasts of future orders for Communications Hubs and Communication Hub Auxiliary Equipment.	Forecasting and ordering of Communications Hubs and auxiliary equipment UC_CSPOMS_001	Full

		Manage the verification of User identities requesting login access to SSI and DCC	Log In UC_Login_001	Full

BFD14	User Identity & Login Access Management	Platforms. Manage the functionality available to individual Users based on their User Role. This includes the following capabilities: • Enable Users to use DCC Identity Provider Service to assign access to functionality to their User Personnel based on Job Type Role and manage the SSI accounts and associated settings (e.g. password resets) for User Personnel accounts subsequently created by an Administration User. • Enable Administration Users to unlock, delete and manage the details of another account created within their organisation. • Enable an Administration User to create a new account for User Personnel within their organiszation. • Enable User Personnel to view detailed information about the account they are accessing via SSI including the functionality they have access to. Ensure secure communications between DCC systems and Users.	User account management UC_OrgManager_001, UC_OrgManager_002, UC_OrgManager_003	Conditional. Access shall be granted to Administration Users.
			User profile information UC_Profile_001	Full

Where a User is entitled to conditional access to more than one Functional Component, the DCC shall apply permissions such that any User Personnel can access any of those Functional Components that the User is eligible to access, subject to such User Personnel being entitled to such access on the basis of the Job Type Role(s) as further set out in 1.5.2.

1.5.2 Administration User defined access

In addition to the full and conditional access restrictions applied by the DCC in 1.5.1, Administration Users, appointed in accordance with the process set out in the DCCKI RAPP, may further define access restrictions for User Personnel to individual Functional Components by assigning one or more Job Type Roles to User Personnel in relation to one or more User IDs. Where a User is using the DCC Identity Provider Service, the DCC shall enable an Administration User to do this through the use of the Functional Component User Account Management.

The DCC shall ensure that access to Functional Components is only provided to the Job Type Role(s) presented to the DCC by the User in the SAML assertion accompanying the request for access to the Functional

Component, on the basis of the Functional Components that the Job Type Role is entitled to access as set out in the table below.

The table below shows which Functional Components that User Personnel with a given Job Type Role are only permitted to access (User Personnel with a given Job Type Role may only access those Functional Components where there is a 'Y' in the corresponding box).

Where the SAML assertion presented to the DCC when seeking to access the Functional Component(s) contains multiple Job Type Roles, the DCC shall grant access to that User Personnel to all of the Functional Components that it is entitled to access in all of those Job Type Roles.

	Job Type Role										
Functional Component	**All Access**	**Organisational Administrator**	**Security User**	**Lead Agent**	**Call Centre User**	**MI User**	**Service Management User**	**Smart Meter Operations User**	**Asset Management Ordering**	**SEC Contract Manager**	**Logistics**
BFD01 Service Management											
Raise service management incidentsUC_RaiseSMI_001 UC_RaiseSMI_002 UC_RaiseSMI_003 UC_RaiseSMI_004	Y	Y	Y	N	N	N	Y	N	N	N	Y
Update service management incidents UC_UpdateSMI_001	Y	Y	Y	N	N	N	Y	N	N	N	Y
View service management incidents UC_ViewSMI_001 UC_ViewSMI_002	Y	Y	Y	Y	N	N	Y	Y	N	Y	Y
Problem management UC_ProblemManagement_001, UC_ProblemManagement_002	Y	Y	Y	Y	N	N	Y	Y	N	Y	Y
BFD02 Smart Metering Inventory											

Smart metering inventory UC_Inventory_001, UC_Inventory_002	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y
BRD03 DCC Service Status											
DCC service status UC_ServiceDashboard_001	Y	Y	Y	Y	Y	N	Y	Y	N	N	N
BDF04 Service Audit Trails											
Service audit trails UC_ServiceAudit_001, UC_ServiceAudit_002	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	N
BFD05 Forward Schedule Of Change											
Forward schedule of change UC_Schedule_001, UC_Schedule_002, UC_Schedule_003	Y	Y	N	Y	Y	N	Y	Y	N	N	N
BFD06 Meter Read Transactions											
Meter Read Transactions UC_Inventory_001	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	N
BFD07 CSP SMWAN Network Coverage											
SM WAN network coverage UC_CSPCoverage_001 UC_CSPCoverage_002	Y	Y	N	Y	Y	Y	Y	Y	Y	N	Y
BFD08 DCC Service Alerts											
DCC service alerts UC_ServiceAlerts_001, UC_ServiceAlerts_002	Y	Y	N	Y	Y	N	Y	Y	N	N	N
BFD09 Service Requests											
Service catalogue publication and call offUC_ServiceCatalogue_001, UC_ServiceCatalogue_002, UC_ServiceCatalogue_003	Y	Y	N	Y	N	N	N	N	Y	N	Y
BFD10 Communications Hub Availability & Diagnostics											
Communications Hub availability and	Y	Y	N	Y	Y	N	Y	Y	N	N	Y

diagnostics UC_HubStatus_001 UC_HubStatus_002											
BFD11 Reporting											
Reporting UC_Reports_001	Y	Y	N	Y	N	Y	N	N	N	Y	Y
BFD12 Knowledge Management, Search and FAQ											
Knowledge management UC_KnowledgeManagement_001	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y
FAQsUC_FAQ_001	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y
DCC user manuals UC_Manuals_001	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y
UC_Search_001	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y
BFD13 Forecasting and Ordering											
Forecasting and ordering of Communications Hubs and auxiliary equipment UC_CSPOMS_001	Y	Y	N	N	N	Y	N	N	Y	N	Y
BFD14 User Identity & Access Management											
Log InUC_Login_001	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y
User account management UC_OrgManager_001 , UC_OrgManager_002 , UC_OrgManager_003	N	Y	N	N	N	N	N	N	N	N	N
User profile information UC_Profile_001	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y

1.5.3 Users granting access to other Users

Information available through the Self-Service Interface that relates to one or more User IDs of a User may be shared with another User where that other User is also willing to share information relating to one or more of its User IDs with the first User.

Where two Users wish to grant access to each other's information accessible through the Self-Service Interface, each of those Users shall submit, via secured electronic means, a notification to the DCC which includes:

- that the notification relates to granting to another User access to its data which is available via the Self-Service Interface;

- the list of User IDs of both of the relevant Users, for which mutual access for the two Users is being granted; and
- details of the DCCKI SRO responsible for the relevant User IDs that is authorising such access on behalf of the User submitting the notification, which shall comprise:
  - the name of the authorising DCCKI SRO;
  - telephone and email contact details for the DCCKI SRO; and
  - signature of the DCCKI SRO.

Upon receipt of such notifications, the DCC shall confirm if each request is authentic, by:

- verification of the DCCKI SRO; and
- by confirming that the User IDs provided by each User granting access are User IDs that have been assigned to each such User by the Panel in accordance with H1.6.

Where both of the notifications are confirmed to be authentic, the DCC shall:

- configure the Self-Service Interface to enable any Administration User acting on behalf of either of the two Users to grant access to its User Personnel to information available via the Self-Service Interface relating to any of such User IDs; and
- confirm in writing, to each DCCKI SRO submitting a notification that such access has been granted.

Where either or both of the notifications are not confirmed to be authentic, the DCC shall confirm in writing, to each of the DCCKI SRO submitting a notification, that such access has been rejected and giving the reasons for rejection.

1.5.4 Users rescinding access permission to other Users

Where a User wishes to rescind permission to allow another User to access its information available through the Self-Service Interface for a defined set of User IDs, having previously granted such access, the User wishing to remove access shall submit, in writing via secured electronic means, a notification to the DCC which includes:

- that the User wishes to rescind access to its information on the Self-Service Interface by another User;
- the list of User IDs pertaining to the User submitting the notification, for which it wishes to rescind access to another User (each a “Rescinding User ID”);
- the list of User IDs pertaining to the other User for which access is to be rescinded (each a “Rescinded User ID”); and
- details of a DCCKI SRO that is authorising such rescinding of access on behalf of the User submitting the notification, which shall comprise:
  - the name of the authorising DCCKI SRO;
  - telephone and email contact details for the DCCKI SRO; and

- signature of the DCCKI SRO.

Upon receipt of such a notification, the DCC shall confirm if the request is authentic, by:

- verification of the DCCKI SRO; and
- by confirming that the User IDs provided by the User notifying that access should be rescinded, are User IDs that have been assigned to that User by the Panel in accordance with H1.6.

Where the notification is confirmed to be authentic, the DCC shall:

- configure the Self-Service Interface to remove access to information relating to Rescinding User IDs by any User Personnel of the second User who were permitted to access such information only by virtue of themselves being permitted to access information relating to a Rescinded User ID;
- configure the Self-Service Interface to remove access to information relating to Rescinded User IDs by any User Personnel of the first User who were permitted to access such information only by virtue of themselves being permitted to access information relating to a Rescinding User ID; and
- confirm in writing, to the DCCKI SROs of both affected Users that such access has been rescinded.

Where the notification is not confirmed to be authentic, the DCC shall confirm in writing, to the DCCKI SRO, that the notification of permission to be rescinded has been rejected.

Version AI 3.0

Appendix AI

Self-Service Interface Code of Connection

Contents

Definitions

In this document, except where the context otherwise requires:

- expressions defined in Section A1 of the Code (Definitions) have the same meaning as is set out in that Section;
- the expressions in the left hand column below shall have the meanings given to them in the right hand column below; and
- any expressions not defined here or in section A1 of the Code have the meaning given to them in the Self-Service Interface Access Control Specification, the SSI Baseline Requirements Document or the DCC User Interface Specification.

Administration User	means, in relation to a particular User, a member of User Personnel who has been appointed to act in such a role in accordance with the DCCKI RAPP (and who has not subsequently ceased to carry out such a role).
Administration User Credentials Request	has the meaning given to that expression in the DCCKI RAPP.
Identity Provider Service	means a service that authenticates that an individual member of User Personnel is who they purport to be for the purposes of access control.
Network Address Translation	means a mechanism by which Users map one Self-Service Interface IP address space to another by modifying network address information in Internet Protocol (IP) datagram packet headers while they are in transit across a traffic routing device.

Personnel Authentication Certificate	has the meaning given to that expression in the DCCKI Certificate Policy.
Policy Enforcement Point (PEP)	a logical entity that enforces policies for admission control and policy decisions in response to a request for access. It is the logical boundary between the DCC Systems and connecting systems, namely User Systems, RDP Systems or any other systems used to access the Self-Service Interface. The PEP ensures that: the policies in the applicable Code of Connection relevant to the applicable Party or RDP are being enforced; there is appropriate separation of the DCC Systems from the connecting systems of the applicable Party or RDP; and all the connections to the User Systems, RDP Systems, systems used to access the Self-Service Interface, or DCC Systems are compliant with the same applicable Code of Connection.
Supported Web Browser	Internet Explorer versions 9, 10 and 11, and a minimum of 2 other browsers as listed on the DCC Website (such list as updated from time to time).
TLS	means transport layer security in accordance with the relevant SMKI PMA and SSC Guidance (Standards, Procedures and Guidelines) published on the SEC website.
UI DCCKICA Certificate	has the meaning given to that expression in the DCCKI Certificate Policy.
Uniform Resource Locator (URL)	a reference to a resource that specifies the location of the resource on a computer network and a mechanism for retrieving it.
W3C WCAG AA	means the World Wide Web Consortium's (W3C) Web Content Accessibility Guidelines (WCAG) for making content accessible. AA is one of three conformance levels.

1. SELF-SERVICE INTERFACE CODE OF CONNECTION

1.1 These provisions apply to the DCC and any User seeking to access information via the Self-Service Interface as described in Section H8.16 of the Code.

General Obligations

1.2 The DCC and each User shall inform each other of the contact details of one or more persons working for their respective organisations for the purposes of communications associated with the use of the Self-Service Interface (in the case of the User, where the contact details for such persons are not already held by the DCC). The following information shall be provided in relation to each such person (and subsequently kept up to date by the Party and/or the DCC):

(a) contact name;

(b) contact email;

(c) contact telephone number;

(d) contact address; and

(e) any other contact details as may be reasonably required by the DCC or the User from time to time.

Restrictions on Physical Connections

1.3 Each User shall only access the Self-Service Interface over a DCC Gateway Connection.

1.4 Each User acknowledges that use of a DCC Gateway Connection for the purposes of accessing the Self-Service Interface will utilise some of the available bandwidth of that connection and may consequently reduce the rate at which information may be exchanged when accessing other Services over that connection.

Connection Mechanisms

1.5 Each User shall route all communications to the Self-Service Interface through its Policy Enforcement Point.

1.6 The DCC shall make the Self-Service Interface available on a set of Internet Protocol version 4 addresses.

1.7 The DCC shall provide details of the set of IP addresses and network configuration to each User, via secured electronic means, as part of the process for obtaining a connection to the Self-Service Interface.

1.8 Each User shall use Network Address Translation to map internal Internet Protocol addresses to the published DCC provided IP addresses within the User's firewall prior to accessing the Self-Service Interface.

1.9 Each User shall use Network Address Translation to remap incoming DCC traffic Internet Protocol addresses from the published IP addresses within the User's firewall to IP addresses within their subnet, as notified by the DCC via secured electronic means.

1.10 Each User shall establish a TLS connection between their User Personnel browsers and either the Self-Service Interface or an Identity Provider Service, in accordance with clause 1.14.

1.11 The DCC shall provide access to the Self-Service Interface to each User using a Supported Web Browser with a minimum screen resolution of 1280x1024 pixels.

1.12 The DCC shall provide reasonable notice to Users of changes to the list of Supported Web Browsers.

Communications Authentication

1.13 Each User shall install a valid Root DCCKICA Certificate, UI DCCKICA Certificate and Personnel Authentication Certificate in its User Personnel's browser prior to establishing a TLS connection to the Self-Service Interface in accordance with the Self-Service Interface Access Control Specification, where such DCCKI Certificates shall be obtained as set out in the DCCKI RAPP.

1.14 The User shall secure the connection between its User Personnel browser and the Self Service Interface or the Identity Provider Service used by the User, using TLS in accordance with RFC5246 and will make use of:

(a) for the Identity Provider Service, mutual authentication using PKCS #3 Ephemeral Diffie Hellman key exchange to generate a shared secret for communications encryption, utilising one of the following cipher suites:

(i) TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256 ECDHE-RSA- AES128-SHA256;

(ii) TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384 ECDHE-RSA- AES256-SHA384;

(iii) TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 ECDHE- RSA-AES128-GCM-SHA256; or

(iv) TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 ECDHE-RSA-AES256-GCM-SHA384; or

(b) for the Self Service Interface, server-side authentication.

Technical Infrastructure

1.15 The DCC shall provide the User, via secured electronic means, with details of a Uniform Resource Locator (URL) to access the Self Service Interface, corresponding with each applicable IP address provided in accordance with clause 1.7.

1.16 The DCC shall give reasonable advance notification to each User of any changes to the Self-Service Interface URL.

1.17 The DCC shall ensure that the IP addresses of the Self-Service Interface shall remain static.

Use of DCC Identity Provider Service

1.18 Each User using the DCC Identity Provider Service shall follow the processes set out in the DCCKI RAPP in order to obtain Personnel Authentication Certificates for its User Personnel prior to accessing the Self-Service Interface.

1.19 Each User that elects to use the DCC Identity Provider Service may create, modify or remove accounts for its User Personnel using the Self-Service Interface as further set out in the Self-Service Interface Specification, save that in the case of accounts for an Administration User, the DCCKI Registration Authority shall, upon receiving an Administration User Credentials Request as set out in the DCCKI RAPP, create, modify or remove the accounts.

1.20 The DCC shall provide an Identity Provider Service that shall, pursuant to clause 1.26, store secure cookies on each User Personnel's browser(s) to validate login sessions and shall ensure that such cookies do not include storage of information that permits personal identification.

Use of an Identity Provider Service that is not the DCC Identity Provider Service

1.21 The DCC shall only permit the use of an Identity Provider Service which conforms to the Identity Provider Service requirements set out in the Self-Service Interface Access Control Specification. The DCC shall not provide access to the Self-Service Interface where a User uses an Identity Provider Service that does not conform to such requirements.

1.22 When using an Identity Provider Service that is not the DCC Identity Provider Service, a User shall provide to the DCC the following details of its authentication arrangements:

(a) identity provider – <name of external Identity Provider Service>; and

(b) identity provider - <External Identity Provider Service URL>

and shall inform the DCC if the details change.

1.23 Each User that elects to use an Identity Provider Service that is not the DCC Identity Provider Service shall ensure that the SAML assertions, as set out in the Self-Service Interface Access Control Specification, are applied to access requests prior to establishing a TLS session.

1.24 Where a User elects to operate an Identity Provider Service that is not the DCC Identity Provider Service, the DCC shall regard an authentic signature on the SAML token for a member of User Personnel as confirmation that the User has appropriately performed verification, validation, role assignment and authentication of that member of User Personnel.

Interface Usage

1.25 Each User shall not use any systems to apply automated tools in order to interact or operate with the Self-Service Interface.

1.26 Each User shall configure each User Personnel's browser to enable the storage of cookies by the DCC in the browser's cookie store.

1.27 Each User consents to the recording and storage by the DCC of details that they make available to the DCC through SAML authentication and request parameters for the purposes of auditing, diagnostics and capacity planning.

1.28 Each User agrees to the recording and storage by the DCC of requests processed by the Self-Service Interface for the purposes of auditing, diagnostics and capacity planning.

1.29 The DCC shall ensure that the Self-Service Interface complies with the W3C Web Content Accessibility Guidelines at an 'AA' conformance level ("W3C WCAG AA").

1.30 The DCC shall log information associated with all requests processed by the Self- Service Interface. Logged information includes data such as the User Personnel's organisation, the User Personnel's username, the URL requested and any inputs provided.

1.31 The DCC shall, upon request, make available to a User, reports summarising the information in clause 1.30 in relation to that User's User Personnel.

1.32 Prior to first use of the Self-Service Interface or where there are any material changes to the following information, each User shall estimate and notify to the DCC:

(a) maximum total active User Personnel accounts;

(b) maximum number of User Personnel concurrently accessing the Self- Service Interface;

(c) average activity (requests/hour/account) for a typical Working Day; and

(d) maximum peak activity in relation to each User Personnel account (the maximum number of requests and the corresponding hour) for a typical Working Day.

Version AJ 4.0

APPENDIX AJ

SEC Variation Testing Approach Document (SVTAD)

Document Control

References

Ref	Title	Source	Date	Version
1	Glossary of Testing Terms	ISTQB	Mar 2016	3.1
2	Joint Test Strategy	DCC	Apr 2015	3.5
3	Testing Issue Resolution Process	DCC	Sept 2015	1.0
4	Joint Test Methodology[1]		Pending Publication	3.0

Table 1 – References

Where this document references sections of the Smart Energy Code (SEC), those references shall be construed by reference to any intended future variations to those Sections (and the SEC Subsidiary Documents associated with those Sections) which are due to take effect at Release 2.0 Go Live as specified by the Secretary of State.

Abbreviations & Acronyms

This document uses standard testing terminology but for the avoidance of doubt, the meanings of abbreviations and acronyms are shown below.

Abbreviation	Meaning
BAT	Business Acceptance Testing
BEIS	Department for Business, Energy & Industrial Strategy
CHTS	Communications Hub Technical Specification
CSP	Communications Service Provider
CTSD	Common Test Scenarios Document
DBCH	Dual Band Communications Hub
DCC	Data Communications Company
DIT	Device Integration Testing
DSP	Data Service Provider

[1] JTM is a methodology agreed by BEIS and industry participants for repeatable laboratory testing of HAN radio performance

FAT	Factory Acceptance Testing
GIT	GB Companion Specification Interface Testing
HAN	Home Area Network
IRB	Issue Resolution Board
ISMS	Information Security Management System
ITCH	Instrumented Test Communications Hubs
OCT	Operational Confidence Testing
PIT	Pre Integration Testing
PTCH	Prototype Test Communications Hub
RDP	Registration Data Provider
SBCH	Single Band Communications Hub
SEC	Smart Energy Code
R2	Release 2.0
RIT	Radio Interface Testing
SIT	Systems Integration Testing
SMETS	Smart Metering Equipment Technical Specifications
SMKI	Smart Meter Key Infrastructure
SM WAN	Smart Metering Wide Area Network
SP	DCC Service Provider
SP UAT	Service Provider User Acceptance Testing
SVTAD	SEC Variation Testing Approach Document

TAG	Testing Advisory Group
TSP	Trusted Service Provider
TTO	Transition to Operations
UEPT	User Entry Process Testing
UIT	User Integration Testing

Table 2 - Abbreviations & Acronyms

Narrative Text

In a number of places this document contains background narrative text, rather than specific rights or obligations (for example in the Introduction section). Whilst not required in the Sec Variation Testing Approach Document, this narrative text is provided for background context for stakeholders.

Glossary

The table below defines only terms that are specifically not as defined in Section A (Definitions and Interpretations) of the SEC[2].

This document uses standard testing terminology, a glossary (Reference 1) of which can be found on the International Software Testing Qualification Board website www.istqb.org

Term	Meaning
1.1 Communications Hubs ("1.1 CHs")	Means single-band and Dual Band Communications Hubs which comply with, or are designed to comply with, the requirements of CHTS v1.1 and GBCS v2.0
DCC Meter Protocol Emulators	Testing Stubs developed by DCC to emulate the functional aspects of smart metering Devices
Modified DCC Total System	Means the DCC System as modified in order to meet (or to be designed to meet) the DCC's obligations under the SEC as at Release 2.0 go live, together with the Communications Hubs that form part of Enrolled Smart Metering Systems.
Instrumented Test Communications Hub	Means a Test Communications Hub that includes an interface making diagnostic information relating to the HAN available. The interface will allow Users to capture HAN activity in real time using a Windows PC.
Release 2.0	Is defined in 1.1 of this document.

[2] https://www.smartenergycodecompany.co.uk/sec/sec-and-guidance-documents

X11 Direction	Means the Secretary of State's direction under section X11 of the SEC dated 23 February 2017, pursuant to which the DCC has prepared this document.
UIT Approach Document	means the User Integration Testing Approach Document for Release 2.0.
User Regression Testing	The regression testing that must be conducted by certain Supplier Parties as described in Section 5 of this document.
Exit Criteria	means the criteria that must be satisfied before testing can be considered complete.
User Testing	means testing by one or more Users of all or part of any changes to the DCC Total System.
User Interface Testing	means the testing that tests the capability of the DCC and the DCC Systems together with the Communications Hubs to interoperate with User Systems.

Table 3 - Glossary

Approval of this Approach Document

The X11 Direction requires that DCC submit this Release 2.0 Testing Approach Document to the Secretary of State for approval after appropriate stakeholder consultation. When submitting the document, DCC will be required to provide the information set out in section X11.6, including why DCC considers the document fit for purpose and details from the consultation process. The Secretary of State will then consider the document, instruct DCC to carry out any remedial actions as necessary and then incorporate the document into the SEC using the powers in Section X5 of the SEC.

As part of the consultation process, the document will be issued to the SEC Panel's Testing Advisory Group and the SEC Panel for review and comment. Any recommendations emerging from this review will be considered by DCC, with amendments made to the document as necessary, and provided to BEIS as per the requirements of section X11.6.

1. Introduction

1.1. General

On 23 February 2017, the Secretary of State directed DCC to produce a Testing Approach document for the changes to the SEC that will be made for the purposes of Release 2.0, in accordance with Section X11 of the Smart Energy Code.

Release 2.0 is defined in the baseline documents agreed by the Technical and Business Design Group on 30 May 2017, as such baseline documents may be updated from time to time, as may the related amendments to the SEC, including the DCC User Interface Specification and Message Mapping Catalogue. These documents are published by SECAS on the 'Developing SEC' page of their website.[3]

[3] https://www.smartenergycodecompany.co.uk/sec/the-developing-sec

Release 2.0 may include additional elements of scope as may be added by DCC itself, which do not affect SEC Parties.

This document sets out the information required of a SEC Variation Testing Approach document in section X11.5 of the SEC, including the manner in which testing will be conducted by DCC as directed for Release 2.0.

1.2. Modification of this Document

This document:

(i) shall be modified by DCC in accordance with any direction to do so made by the Secretary of State;

(ii) may be modified by DCC following consultation with affected parties, the Authority and the Secretary of State, provided that:

(a) prior to making any such modification, DCC must present to the Secretary of State a summary of the consultation responses received and an explanation of how the DCC has taken them into account; and

(b) it may not be modified to the extent that the Secretary of State directs otherwise; and

(iii) may be modified by DCC without consultation where the modification is of a minor typographical nature, or where the modification does not have any material effect on the rights or obligations of SEC Parties or any other person who is entitled to undertake testing in accordance with this document.

2. Scope

In plain terms, Release 2.0 will update the DCC Total System to support updated versions of key technical smart metering specification documents. It will see DCC introduce new Communications Hubs with additional radio capabilities (Dual Band Communications Hubs) that will enable Supplier Parties to install Smart Metering Systems in an increased proportion of GB homes. In addition, it will see DCC provide updated single band Communications Hubs and upgrade existing Single Band Communications Hubs to reflect amendments and clarifications in the Release 2 requirements. Further, all CHs will need to support current and updated versions of the ZigBee Alliance specifications and the Devices that use them.

This will be the first Release to introduce new Devices to the DCC Total System that operate to different device specifications. As a consequence, the DCC Total System will need to support Devices operating on multiple technical specification standards.

As for earlier Releases (R1.x), DCC will perform testing following established industry practice. The changes will be developed and tested by DCC Service Providers, then subjected to integration testing by DCC and then made available to Parties for integration testing with their Systems and Devices.

This approach document describes how this testing will be conducted and assured to make sure the changes fully meet the new requirements and obligations, at the same time as ensuring that the changes do not undermine the ability of Parties to continue to meet their existing obligations.

The document describes the objectives of testing and defines the different stages of testing in terms of the activities, resources and evidence needed to meet those objectives.

All 1.1 CHs variants will be subject to testing in R2.0.

In addition to, and supporting the specific direction received from the Secretary of State, Release 2.0 includes changes to the following components of the DCC Total System/Services;

- GIT for Industry (GFI Testing under section X9 of the SEC)
- DCC Meter Protocol Emulator (see 13.2 below)
- Parse & Correlate Software
- DCC enterprise systems (the systems which support the usage, billing and reporting of use of DCC Services)
- Instrumented Test Communications Hubs (see section 13.3.3)

Where this document places an obligation on any DCC Service Provider, or any personnel of a DCC Service Provider, it shall, for the purposes of the SEC, be read as an obligation on DCC to ensure that the relevant Service Provider meets that obligation.

2.1. Documents for Release 2.0

The table below lists the specifications that were notified to DCC for implementation in Release 2.0.

Document Name	Version
Smart Metering Equipment Technical Specification (SMETS2)	v3.0
Communication Hub Technical Specification (CHTS)	v1.1
GB Companion Specification (GBCS)	v2.0

Table 4 - Technical Specification

2.2. Joint Testing Strategy and Other DCC Testing Approach Documents

For Release 1.2 and 1.3 DCC produced a Joint Testing Strategy and a number of individual Testing Approach documents covering separate testing phases and activities. These documents established processes, reports and other elements that are now ongoing elements of DCC activities.

The Joint Testing Strategy has not been updated to reflect developments and improvements resulting from the delivery of Release 1.x and large parts of other Testing Approach documents are similarly no longer applicable.

Where relevant, or where there is an apparent conflict with the Joint Testing Strategy and other Testing Approach Documents developed for Release 1.x, this Testing Approach Document for Release 2.0, and relevant Approach Documents for Testing Phases, supersede and replace those earlier documents.

Recognising the potential variety of future DCC change, a new high level DCC Testing Principles document will be created to inform and reflect the ongoing change activities, the content of this Testing Approach Document and lessons learned.

2.3. Out of Scope

A number of requirements in this document do not apply for DSP PIT, which is a testing phase planned to be completed ahead of other testing phases and has been designed based on the existing DSP PIT processes and the Joint Testing Strategy. At the time of consulting on this document, DSP PIT has already commenced - DCC considers there to be minimal risk to Parties associated with that development work.

A number of the requirements in this Testing Approach Document do not apply to UIT, which is a Testing Phase to allow Parties to conduct their testing. For instance, the DCC Systems Integrator is not responsible for providing test artefacts for test participants and a separate defect process and repository is used.

The following assurance activities are outside the scope of the testing approach for Release 2.0:

(i) CPA Certification of Communications Hubs (CSPs are responsible for this activity)

(ii) DCC is not responsible for proving that Devices are compliant with SMETS requirements, but will undertake testing with Devices and provide testing services that Parties can use as part of their own Device testing

(iii) Testing of the Home Area Network (HAN) except for:

(a) its interaction with the Modified DCC Total System

(b) where the HAN is tested as part of Device Integration Testing and User Integration Testing

(iv) Testing the inter-changeability of Devices connected to the Home Area Network

3. Objectives of Testing

3.1. Testing Objectives

The following testing objectives are contained in the X11 Direction received from the Secretary of State[4]:

(a) demonstrate that 1.1 CHs designed to comply with CHTS v1.1 do comply with CHTS v1.1 and GBCS v2.0

(b) demonstrate that Communications Hubs that comply with CHTS v1.0 / GBCS v1.0 can be upgraded to comply with CHTS v1.1 / GBCS v2.0 via a firmware upgrade sent over the SM WAN

(c) demonstrate that DCC and the component parts of the Modified DCC Total System together with 1.1 CHs operating to CHTS v1.1 / GBCS v2.0 technical specifications operate and interoperate with each other, and with User Systems and RDP Systems, to the extent necessary that DCC and RDPs are capable of complying with their obligations under Sections E (Registration Data), G (Security), H (DCC Services) and L (SMKI) (and for such purposes DCC shall, to the extent reasonably practicable, use Devices that comply with (or have been designed to comply with) SMETS2 v3.0

(d) demonstrate the extent to which the Modified DCC Total System and both new 1.1 CHs and those upgraded from CHTS v1.0 are capable of interoperating:

[4] Note that the definition of DCC Total System in the direction is that as modified to include changes for Release 2.0. This is reflected in the use of the term Modified DCC Total System in this document.

(i) with the Device or Devices that form part of an Enrolled Smart Metering System; and

(ii) with IHDs that have been installed pursuant to Condition 34 or 40 of (respectively) the Electricity Supply Licences or the Gas Supply Licences

in each case where one or more of those Devices comply with SMETS2 v2.0 (but not SMETS2 v3.0)

(e) enable (to the extent that it is reasonably practicable to do so, and in each case as far as reasonably practicable in advance of Service Release 2.0 Go Live):

(i) Parties to test the interoperability of their User Systems with the DCC System together with 1.1 CHs; and

(ii) Testing Participants to test the interoperability of Devices that comply with (or have been designed to comply with) the requirements of SMETS2 v3.0 with the DCC System together with 1.1 CHs

(iii) Demonstrate that the new versioning aspects of the DUIS operate correctly for Users to facilitate communication to a mixed estate of Devices operating to multiple different technical specifications with different functionality sets

(iv) Demonstrate that Users can successfully install and commission and operate all Communications Hubs using the Modified DCC Total System

In addition, the following testing objectives shall also apply:

(f) demonstrate that the Modified DCC Total System can operate successfully within a wider Smart metering ecosystem comprised of multiple Devices operating to different technical specifications in a consistent manner;

(g) test end-to-end communication from User to Device and back again for all technical specifications in operation, together with the updated Parse and Correlate Software;

(h) verify that all other functional changes that are part of Release 2.0 are functionally correct including consequential amendments (e.g. anomaly detection);

(i) throughout the process, testing will be in accordance with Good Industry Practice, and with wider DCC objectives in Condition 5 of the DCC Licence;

(j) wherever practicable, use of automated testing is required to improve the efficiency and lower the cost of testing;

(k) assure Single Band Communications Hubs and Dual Band Communications Hubs against v3.0 of the Joint Test Methodology;

(l) ensure that the changes do not materially impact the security risks associated with the Modified DCC Total System, or changes are identified, tested and accepted. Consideration should be given to the security capabilities in the DCC security architecture including the protection of data and infrastructure;

(m) validation, as defined in specific Test Phase Approach Documents, of all DCC operational impacts and regression testing of the service to ensure continuity; and

(n) validation, as defined in specific Test Phase Approach Documents, of the end-to-end data flows via the Modified DCC Total System (including reporting).

(o) In pursuance of objective c above, all Communications Hub variants will be subject to testing in R2.0 to evidence that:

(i) R2.0 development has not introduced any unintended capability regression from existing functional or non-functional behaviours such that backward compatibility is assured

(ii) New or modified functional or non-functional behaviour which is required for the Modified DCC Total System in order to meet the R2.0 requirements has been developed and implemented and is fit for purpose

(iii) Where practicable, overall Communications Hub behaviours are consistent between variants across the CSP Regions

In respect of the testing objectives described above:

(a) references to the SEC shall be construed as a reference to the intended future version of the SEC (including any Subsidiary Documents) which are due to have effect at Release 2.0;

(b) the testing objective shall be read as an objective to demonstrate or enable (as the case may be) testing of any particular thing only to the extent that such thing has not already been demonstrated or enabled by previous testing under the SEC;

(c) the testing objective shall include the regression testing of existing key end-to-end processes to ensure that they are able to operate under both Release 2.0 and previous releases;

(d) the testing objective may be met in multiple stages; for example, meeting it separately in relation to single-band and then Dual Band Communications Hubs; and

(e) the testing objective may be met in parallel with meeting the testing objective of other changes to DCC Systems.

3.2. Technical Specification Versioning

Release 2.0 of the DCC Systems will be the first release of the DCC Systems that will support Devices that may comply with different versions of GBCS, SMETS and CHTS according to the entry for the Device Model in the Certified Products List.

The introduction of updated technical documents means that Devices within the smart metering ecosystem can have different features and functionality while still being conformant to the regulation and be interoperable with other Devices conformant with a different set of technical documents. The Modified DCC Total System for Release 2.0 has to operate successfully to support communication to all Devices regardless of which applicable technical documents they are conformant with.

The DCC User Interface and the rest of the Modified DCC Total System shall therefore support multiple versions of technical documents across the mixed estate of Devices that will exist within the smart metering eco-system at any point in time.

DCC will provide information for Users on the process steps involved to operate with DUIS v2.0.

Release 2.0 of the DCC Systems introduces an upgrade to the DCC User Interface Specification (DUIS) and enables, for the first time, User choice regarding which version of DUIS they wish to operate against, v1.0 or v2.0. A User may only operate against a single version of DUIS at any one time.

Backward compatibility of GBCS use cases in versions of GBCS with a valid Applicability Period must be supported by the DCC User Interface and the rest of the Modified DCC Total System (unless specifically mandated otherwise within GBCS for a specific GBCS Use Case). The latest version of DUIS will support Devices with older GBCS versions as well as the Devices compliant with the latest GBCS version.

Forward compatibility, meaning use of DUIS v1.0 with a Device that is compliant with GBCS v2.0, shall be supported by DCC for GBCS use cases that are in common between GBCS v1.0 and GBCS v2.0.

It shall not be possible for a Service Request issued by a User to DCC via DUIS v1.0 to be transformed by the Modified DCC Total System into a GBCS Command/message code which has been newly introduced in GBCS v2.0.

The upgrade to DUIS v2.0 is optional for Users however if any of the v2.0 functionality is required, it will be necessary for the User to upgrade.

It is expected that some Users will want to test the new DUIS v2.0 (functionality and regression) and some Users (not upgrading to DUIS v2.0) will want to regression test against DUIS v1.0. Some Users may wish to undertake both activities.

DCC will test technical specification versioning during the DSP PIT and SIT test phases.

Testing during these phases shall demonstrate that the new versioning aspects of the DUIS operate correctly to allow Users to communicate, using their preferred version of DUIS, to a mixed estate of Devices operating to multiple different technical specifications with different functionality sets.

The following are key principles for DUIS versioning (DUIS versions and GBCS versions):

- The old DUIS v1.0 remains supported by DCC and continues to support all the use cases in GBCS v1.0.
- The new DUIS v2.0 needs to support Devices running both old and new versions of GBCS.
- The old DUIS version can be used with updated Devices where existing GBCS use cases are still supported in the later GBCS version.
- DUIS v1.0 cannot be used to access use cases that appear in GBCS v2.0 but not in GBCS v1.0
- A User should plan to operate against a single version of DUIS, either DUIS v1.0 or DUIS v2.0

Users, as part of UIT, will be able to test with the new DUIS versioning functionality to ensure that the Modified DCC Total System is working correctly as designed against the version of DUIS that they intend to use upon implementation of Release 2.0. Users will be able to test Service Requests in UIT against their chosen DUIS version against a mixed estate of Devices operating at different GBCS versions to ensure that commands are processed as expected and appropriate Responses received correctly by Users.

4. Testing Approach

As described above, Release 2.0 comprises changes to support the increment of a number of baseline technical documents, the introduction of Dual Band Communications Hubs and any changes to the DCC Systems and processes needed to support the release.

The scope of the DCC Total System that relates to processing communications with Users and Devices is shown below (in the grey box + the HAN).

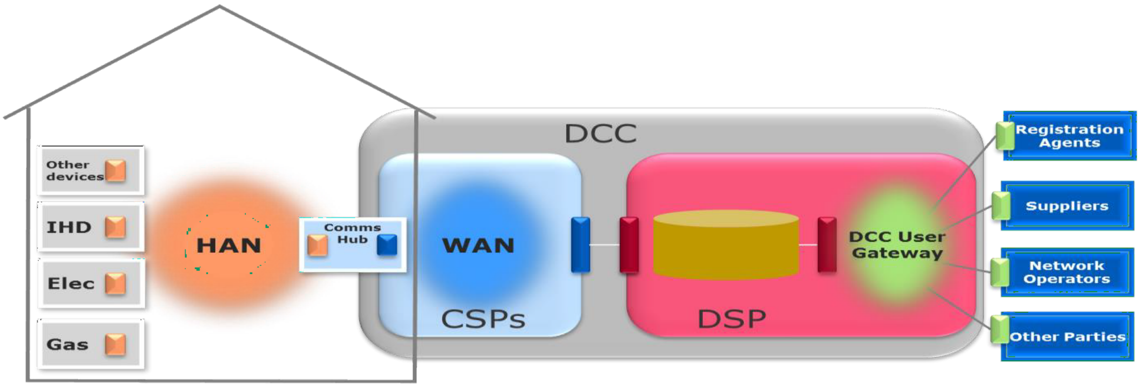


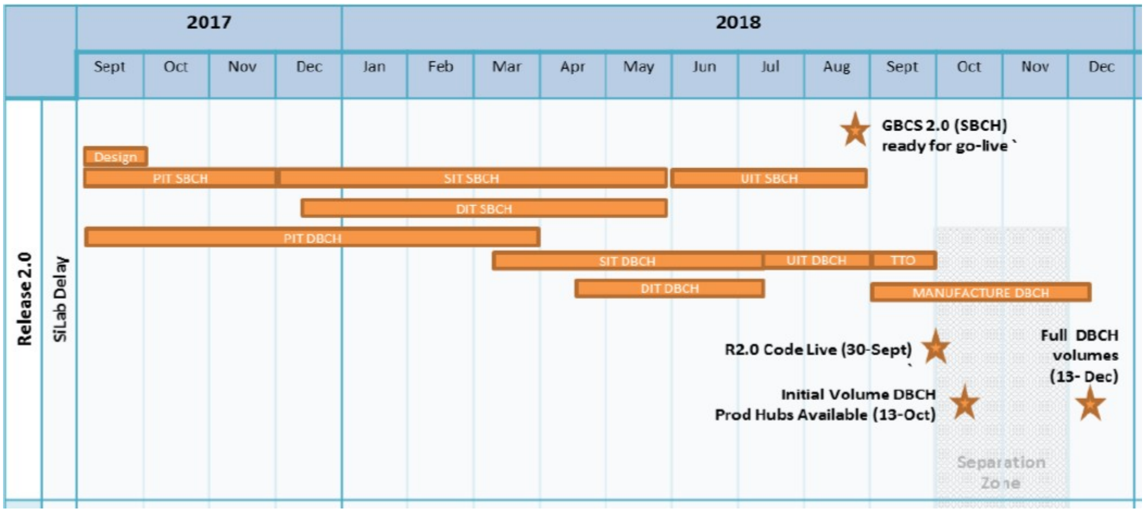
Figure 1 – Scope of DCC Total System for Processing Service Requests

All interfaces and functions of the Communications Hub, including the HAN interface and Gas Proxy Function, fall within the scope of the DCC Total Systems. The Parse and Correlate Software is also part of the scope of the DCC Total System.

This document will describe the specific testing approach requirements for each phase, and then describe the common approach requirements that apply across the release.

4.1. High Level Plan

The detailed delivery plan is described in the Licence Condition 13 planning document for Release 2.0 and is not included in this Testing Approach Document. A high level outline plan is shown below.



The changes that comprise Release 2.0 will be developed and tested by DCC and its Service Providers in three parts. All parts will include regression testing and backwards compatibility testing.

- Part 1 – Early Integration (DSP Only). Regression testing of the R1.3/1.4 functionality by DSP only for backwards compatibility, plus testing of new DSP functionality to support a Device estate operating to multiple different versions of technical specifications with a CSP simulator.
- Part 2 – GBCS v2.0 testing with a Single-Band Communications Hub compliant to CHTS v1.1 for all Service Providers. Testing of new GBCS v2.0 functionality between DSP and CSPs.
- Part 3 – GBCS v2.0 testing with a Dual Band Communications Hub compliant to CHTS v1.1 for all Service Providers. Testing to complete the scope of Release 2.0.

4.2. Description of Test Phases

The approach to testing will include defined test phases. Subject to 4.3 below, and accepting an overarching principle for Release 2.0 to progress testing from phase to phase iteratively to facilitate progress and provide access to Parties for testing earlier than waiting for a test phase to complete, these are steps to develop and assure code or products prior to making them available in production.

In plain English, and with further detail provided in section 5 below, the test phases can be described as follows:

- The Pre Integration Test (PIT) phase covers the testing by DCC Service Providers undertaken individually to verify that the solution meets the requirements
- Systems Integration Testing (SIT) confirms that the different DCC Service Provider and DCC internal systems work effectively together to meet the requirements of the SEC and operate as a working system for Users. This phase will include
- Solution Testing and Service Provider User Acceptance Testing (SP UAT). It will also include Operational Confidence Testing by the DCC Service Providers.
- Device Integration Testing (DIT) will test the interoperability between the Modified DCC Total System and 1.0 CHs, new 1.1 CHs (Single and Dual Band) and those that have been upgraded from CHTS v1.0 and
  - Devices that form part of Enrolled Smart Metering Systems and associated IHDs; and
  - new Devices complying with SMETS2 v3.0 (where Devices are available to support testing)
- DIT will take place independently of other phases, and will be subject to the overall LC13 plan, but is expected to be undertaken at the same time as SIT. The start of DIT will be offset from the start of SIT to ensure that components integrate prior to beginning testing with Devices.
- User Integration Testing (UIT) allows Users to test their systems and Devices with the Modified DCC Total System before changes are made available in the production environment. For Release 2.0, each Supplier Party that is a Responsible Supplier for any Device with an SMI Status of ‘commissioned’ is required to execute User Regression Testing against the Modified DCC Total System, as further described in Section 5. UIT also allows new and existing Parties to provide evidence of their ability to interact with the Modified DCC Total Systems for formal user testing using DCC Meter Protocol Emulators.

- Testing to support the Transition to Operations (TTO). These testing stages may operate independently and overlap with other phases. Testing as part of this group will include Operational Acceptance Testing, Business Acceptance Testing, security testing, pre-production proving and any required Performance Testing. It is the phase that assures that DCC Systems and processes – including billing and reporting are ready to support the changes introduced by the wider release.

The table below shows how the test phases address the testing objectives (using summarised language) described in detail above in section 3.1.

Ref	Objective	Test Phase
A	Demonstrate that new 1.1 CHs comply with CHTS v1.1	CSP PIT, SIT
B	V1.0 Communications Hubs can be upgraded to comply with CHTS v1.1 and GBCS v2.0	CSP PIT, SIT
C	Demonstrate that Modified DCC Total System together with v1.1 CHs interoperate with each other and User Systems to comply with SEC	CSP PIT, SIT, UIT, DIT, TTO
D	Regression testing for existing Devices and new SMETS2 3.0 Devices	PIT, DIT, SIT
E	Support User testing of Systems and Devices	UIT
F	Good Industry Practice and DCC objectives	PIT, SIT, UIT, DIT, TTO
G	Use of automated testing	PIT, SIT
H	Assure the 2.4GHz and Sub GHz RF Coverage performance	CSP PIT
I	Security	PIT, SIT, UIT, TTO
J	Communications Hubs work as intended	CSP PIT, SIT, DIT
K	DCC operational impact	UIT, TTO
L	End-to-end data flows	PIT, SIT, UIT, DIT

Table 5 Testing Objectives by Phase

Alongside the testing activities associated with Release 2.0, DCC will continue to provide support for testing by new and existing Parties as part of the ongoing provision of testing services.

Release 2.0 changes a live system and will be developed and planned at a time when significant User testing of the system will be taking place within E2E testing. The Release must take account of incidents from production, and issues raised in E2E testing, both in test plans, but also as they arise during test phases.

Security testing should include appropriate testing to demonstrate security of the test and production environments and code. This may include penetration and other vulnerability testing, and may occur across multiple test phases.

DCC shall make available a version of the Parse and Correlate Software that is consistent with the functionality of Devices and DCC Systems that will be in operation from Release 2.0 live in the timescales set out in the Release 2.0 LC13 plan.

4.3. Delivery of Test Phases and Stages

In accordance with the X11 Direction, the execution of the testing to support Release 2.0 may be undertaken in multiple stages, this could include the possible delivery of multiple PIT, SIT and UIT phases, but using the same Release 2.0 PIT, SIT and UIT environments.

The approach may also include overlapping testing phases and stages to support early availability of elements of the scope, but consistently subject to the established DCC quality gating process including the DCC Test Assurance Board.

Apart from SIT and DIT which have been designed to be parallel and concurrent phases (with suitable dependencies for components and service requests to pass in SIT prior to being used in DIT), there will be no parallel testing across phases for any given functionality – functionality will not be released into a subsequent phase until testing, assurance and governance procedures are completed for prior and current test phases. The option to overlap, for instance SIT and UIT, is intended to allow Parties to test the GBSC v2.0 solution in UIT with Single Band Communications Hubs whilst SIT for Dual Band Communications Hubs is ongoing.

The detail of the execution plan for Release 2.0 is contained in the Licence Condition 13 Plan.

5. Supplier Parties – User Regression Testing

Each Supplier Party that is a Responsible Supplier for any Device that has an SMI Status of ‘commissioned’ on the date of the milestone “UIT TSG 2.0/SBCH Commence” (as defined in Table 7 of UIT Approach Document), shall:

(a) take all reasonable steps to meet the Entry Criteria for User Regression Testing, as set out in Section 5.1.1 of the UIT Approach Document, by no later than 50 working days prior to the date of the milestone “R2 End of UIT testing Window” (as defined in Table 7 of the UIT Approach Document);

(b) ensure that in carrying out User Regression Testing it sends test Service Requests that are consistent with Version 0.8.2.1 of the DUIS XML Schema;

(c) ensure that the scope of its User Regression Testing tests comply with the requirements of Section 5.1.3 of the UIT Approach Document;

(d) cooperate with the DCC to ensure that all of its User Regression Testing tests are executed by a date which is no later than 10 working days prior to the date of the milestone “R2 End of UIT testing Window” (as defined in Table 7 of the UIT Approach Document); and

(e) provide the DCC, by the date which is no later than 5 working days prior to the date of the milestone “R2 End of UIT testing Window” (as defined in Table 7 of the UIT Approach Document) , a self-certification of completion of User Regression Testing in the form provided by the DCC.

6. Test Phase Description

This section 6 of the Release 2.0 Testing Approach Document defines the testing activities and assurance requirements for individual test phases.

Subsequent sections describe and define generic elements of the approach to testing for Release 2.0. e.g. roles and responsibilities.

The testing deliverables required in section 8 below shall ensure that these requirements and focus areas are suitably covered by each DCC Service Provider and each testing phase, and assured accordingly. All requirements and deliverables for each phase shall ensure that the test objective coverage described in Table 5 above is met.

6.1. Requirements & Focus Areas for Pre Integration Testing

PIT for Release 2.0 is required to provide assurance of quality earlier in the process than has previously been the case for DCC Releases.

As an overall requirement, any and all testing which can be reasonably and cost- effectively undertaken prior to SIT should be undertaken in PIT.

Ref	Requirement
PIT.1	DCC Test Assurance will engage in PIT across all activities except unit and link testing, as subsequent activities within PIT provide assurance of outputs from those tests
PIT.2	DCC Systems Integrator shall support the DCC Service Provider PIT activities
PIT.3	DCC Service Provider PIT shall include suitable performance testing
PIT.4	DCC Service Provider PIT shall be conducted using the latest available version of Parse and Correlate Software
PIT.5	DCC Service Provider PIT shall include suitable security testing of the whole solution. Specifically for CSPs this will include security testing of their Sub-GHz design and components
PIT.6	CSPs shall use a common methodology to assess the effectiveness of their HAN radio implementation and HAN coverage
PIT.7	Functional testing shall be aligned with all specifications, including CHTS v1.1 requirements
PIT.8	CSP Testing of GBCS v2.0 10.6.2.2 (Duty Cycle Monitoring) shall be undertaken using emulators
PIT.9	DCC shall review and approve the PIT test scenarios, where used, for appropriateness and suitable functionality coverage
PIT.10	CSP to verify ZigBee interPAN functionality

PIT.11	CSP to verify full functionality with maximum Devices attached
PIT.12	CSPs to demonstrate through testing that the WAN coverage assumptions which support the CSP “B” milestones are not jeopardised by the new Dual Band CHs
PIT.13	CSPs to demonstrate through testing that SM WAN connectivity is reliable and robust over a range of timed periods, at different power levels

Table 6 PIT Requirements

6.2. Requirements & Focus Areas for Systems Integration Testing

SIT for Release 2.0 shall be planned to allow for incremental delivery (based on incremental proving out of PIT) of functionality from SIT to support earlier delivery of final, assured code for User testing.

Ref	Requirement
SIT.1	SIT will be undertaken using scenario testing and will ensure that Service Requests are validated for the correctness and consistency of content, alongside the correctness of formatting
SIT.2	SIT coverage will be proved using a test traceability matrix, which may be facilitated by the use of additional reporting tools
SIT.3	SIT will be designed to make use of automation where practicable to improve testing throughput rates
SIT.4	SIT will test all variants of 1.1 CHs, and regression against 1.0 CHs
SIT.5	SIT will include suitable security testing, including protection of data and E2E messaging security
SIT.6	SIT will include Solution Test and Service Provider User Acceptance Testing
SIT.7	SIT will include non-exhaustive testing of disruptive and negative functional test scenarios
SIT.8	SIT shall be performed using assured testing stubs and Meter Protocol Emulators. If there are Devices where there are no assured emulator alternatives, e.g. In Home Displays, then SIT shall use actual Devices
SIT.9	Testing of the integration with the Parse & Correlate Software
SIT.10	SIT will include testing of the Local Command Interface using a hand held terminal Device, or a suitable testing tool developed to emulate connectivity at the Local Command Interface[5]

[5] This interface is only required for the 2.4GHz interface

SIT.11	SIT will include verification of the correct operation of all interfaces in DCC Systems
SIT.12	SIT will include verification that the correct E2E data is contained in all relevant DCC enterprise system produced report feeds
SIT.13	SIT will include suitable tools to allow testing and verification of encrypted and sensitive payloads
SIT.14	Where SIT makes use of the DCC Meter Protocol Emulator, testing must include emulator configuration to provide valid data in a service response. A blank / null response cannot result in a passed test. The response must include valid data that can be successfully parsed and where relevant decrypted, to prove the response data received is as expected based on the emulator configuration for that test
SIT.15	SIT will include appropriate levels of testing of the v1.0 to v1.1 Communications Hub upgrade process to reflect the installed base of v1.0 Communications Hubs
SIT.16	SIT will include testing 1.0 CHs with the Modified DCC Total System

Table 7 SIT Requirements

Specifically for SIT.10, testing of the Local Command Interface shall cover, as a minimum, the following activities:

- Service user simulator to DSP to service user simulator local command
- Local command to Communications Hub Function to Device
- Device to Communications Hub Function to local response
- Local response to service user simulator to DSP

6.2.1 Service Provider User Acceptance Testing

The SIT Phase includes the DCC Service Provider User Acceptance Testing (SP UAT) activity. This activity will operate concurrently with Solution Test, and is undertaken to provide additional assurance.

It allows DCC to witness an agreed subset of the tests carried out in Solution Test. The subset of tests will be described in a SP UAT test plan.

Giving at least 2 Working Days' notice, the DCC Systems Integrator will provide DCC with a schedule of when and where tests will be executed and invite DCC to witness either on- site or remotely.

Witnessing of the test execution, or reviewing evidence of executed tests, will adhere to two key rules;

- There will be no deviation from test scripts
- There will be no hands on execution by witnesses

SP UAT will report on test completion, test failures and test pass rate independently of Solution Test, in order to ensure that 100% coverage and other success criteria of SP UAT are met.

6.2.2 Operational Confidence Testing

At the same time as SIT, and for functionality that has completed SIT, the CSPs will undertake Operational Confidence Testing to assure functionality and non-functional performance of the Communications Hubs, supported by the DCC Systems Integrator and the DSP.

In the absence of a suitable environment for complete non-functional testing, Operational Confidence Testing will address non-functional testing as is practicable, and will include characterisation of timings, testing of different network transport layers and soak testing of Communications Hubs over a range of time periods to identify defects and issues occurring as a result of extended operation, including intermittent HAN connections.

Because of the nature of Operational Confidence Testing a different definition of success criteria will be applied. These will be defined by the Communications Service Providers in a joint OCT approach document and reviewed by the SEC Panel Testing Advisory Group (TAG), but will not be part of the SIT audit scope.

The OCT approach document will include;

- summary scope of tests to be carried out by each CSP
- detail of the environments to be used for OCT
- assurance approach and progress/test coverage reporting
- interaction with the DCC Systems Integrator
- approach to classifying and managing defect
- success criteria and completion report.

Where relevant, Operational Confidence Testing will be coordinated with DIT.

6.3. Requirements & Focus Areas for User Integration Testing

The provision of User Integration Testing environments and associated services is part of DCC's ongoing activities, this section 6.3 describes the specific requirements and focus areas for Release 2.0.

Release 2.0 will introduce a second UIT environment to allow Parties to continue to test against the Release 1.0 code base/production (using the existing UIT A environment) in parallel with testing the Release 2.0 solution (using the new UIT B environment initially). How DCC will operate multiple UIT environments, and how Parties will interact with those environments, will be covered in a new DCC deliverable defined in section 8 below.

DCC shall provide a testing service (User Integration Testing (UIT)) that allows a Party to test the interoperability of its User Systems with the Modified DCC Total Systems (including via the Self-Service Interface), and to test simultaneously the interoperability of User Systems and Devices (other than those comprising Communications Hubs) with the Modified DCC Total Systems and with Test 1.1 Communications Hubs provided by DCC. This testing service shall be made available on the same basis as Testing Services under Section H14 (Testing Services), but subject to this Testing Approach Document.

As for previous releases, there will be a period between the completion of SIT and promoting functionality to live operations. This period allows for Parties to undertake any User Entry Process Testing (UEPT) activities and test with the Modified DCC Total System as they choose. Certain Supplier Parties will also carry out User Regression Testing as described in this Testing Approach Document.

The UIT Approach Document will provide timings for the uplift of DCC documents relating to User Testing, including the options for completing additive UEPT for Release 2.0 and how test Devices should be managed in a multiple environment context.

DCC now operates a production business, and defects found in User testing against DCC Systems will be managed through to resolution by the appropriate DCC release channel available. The Enduring Test Approach Document will be updated to provide detail of this process.

Ref	Requirement
UIT.1	UIT will enable Parties to test Release 2.0 functionality
UIT.2	UIT will be planned to allow earlier availability of functionality from SIT for Parties to test against their systems and Devices, ahead of the completion of the full Release
UIT.3	UIT will include the provision of a Prototype Test Communications Hub for remote test labs, to enable the testing and diagnosis of HAN interoperability and HAN performance
UIT.4	UIT will include the provision of an Instrumented Test Communications Hub for DCC and remote test labs, to allow participants to diagnose and assure HAN performance and interoperability with other Devices, and undertake functional testing[6]
UIT.5	The deployment of new releases to UIT will be subject to specific entry criteria and testing to ensure minimal risk of disruption to ongoing participant testing in the environment
UIT.6	UIT security testing of DCC user authentication and authorisation, including protection of data and E2E messaging security
UIT.7	UIT testing shall include the capability for participants to verify all installation and maintenance activities for CHs as described in the SEC
UIT.8	UIT testing must include the capability for participants to verify their end-to- end data is operating correctly over DUIS and SSI, and in SSI reports
UIT.9	UIT testing must include the capability for DCC operations to verify their processes using SSI, SSMI, and reports as in the production environment but based on actual participant activities

[6] Release 2.0 will introduce a Dual Band Instrumented Communications Hub for use in DCC and remote test labs. A single band Instrumented Communications Hub is subject to a separate DCC Change Request and is not part of Release 2.0. The earlier of the provision of DB ITCH or SB ITCH will see DCC update working practices and testing participant guidance documentation to support the use of ITCH in RTLs as part of overall issue management activities

UIT.10	UIT testing shall allow for users to test with the mesh technology
UIT.11	DCC will make meters available to be requested for testing by Users who are not in a position to install and commission meters themselves – e.g. Network Operator Parties
UIT.12	Supplier Parties with commissioned Devices are required to execute User Regression Testing as described in Clause 5 of this Test Approach Document

Table 8 UIT Requirements

UIT will continue to support UEPT. DCC will propose updates to the Common Test Scenarios Document (CTSD) to reflect the functionality available as a result of Release

2.0. All Parties who have not previously completed UEPT will be required to prove their capability against the full set of relevant requirements in CTSD for the user roles they seek to operate in production.

Existing Users will be required to prove their capability against the updated requirements in CTSD for the User Roles they seek to operate in production. Parties can select whether to follow the documented UEPT process supported by DCC, or provide evidence of their capabilities outside of the documented UEPT process for DCC to consider prior to issuing certificates. UIT for Release 2.0 will be sufficient in scope for Parties to prove their capability to use the new Services.

Full detail of the process and how Parties will be able to engage with DCC to complete UEPT in the manner of their choosing, if they are entitled to choose, will be provided in the UIT Approach Document.

Where a Party provides evidence to DCC that it has proven its capability to use one or more of the new Services and DCC is not satisfied that a Party has successfully demonstrated that capability, that Party may refer the matter to the Panel for its determination (which shall be final and binding for the purposes of the SEC).

It is noted that DCC maintains its obligations to provide and support an integrated environment for the purposes of user testing, which includes ongoing assurance of the provision of CSP and remote test labs used within UIT, and demonstrating that the UIT environment is secure.

6.4. Requirements & Focus Areas for Device Integration Testing

DIT as a phase will build upon the lessons learnt from Release R1.2 and R1.3. During DIT DCC will engage with Device manufacturers throughout and notify Parties of the ongoing DCC interoperability events and other DCC engagement.

The deliverables for this test phase shall acknowledge the potential availability risk of suitable Devices and make exceptional provision for DIT to be undertaken using testing stubs, subject to approval to do so being provided by BEIS.

Further to the lessons from R1.3 testing with meters, DIT will be a formal test phase, and shall be required to achieve 100% coverage of planned tests, rather than be time limited. The exception will be when tests are blocked due to meter defects which are confirmed to exist in the live code base, which are not fixed by meter manufacturers within DIT timescales.

DIT will provide industry with confidence that v1.1 Communications Hubs, and v1.0 Communications Hubs upgraded to v1.1 interoperate with existing SMETS2 v2.0 Devices (including IHDs) and Devices designed to meet SMETS2 v3.0. DIT will also provide industry with the confidence that v1.0 Comms hubs and SMETS2v2 Devices interoperate with the Release 2.0 code base.

DCC has undertaken a documented commercial selection activity to determine which Devices and manufacturers will participate in DIT in line with the requirements below. All selected participants in DIT have confirmed the readiness and suitability of their Devices to support DIT.

All of the requirements below are subject to the availability of sufficient firmware and individual Devices, capable of fully participating in the testing at the time of the planned activity and supported by the manufacturers of those Devices.

If the availability of sufficient capable and supported Devices would result in any of the requirements below being at risk of not being proven, following confirmation with BEIS, DCC will complete such testing as is practical (potentially utilising emulators) and provide detail of the reasons why DIT has not been fully completed in the Test Phase Completion report. DCC will endeavour to complete any coverage of testing with Devices in UIT should suitable Devices become available after the completion of DIT and prior to go live.

DIT will be conducted in the same environment as SIT, coordinated to ensure Device testing scenarios and combinations take place against an appropriate code base.

Ref	Requirement
DIT.1	DIT shall test Communications Hubs with a minimum of 2 ESME Device Models from different manufacturers designed to meet SMETS2 v3.0
DIT.2	DIT shall test Communications Hubs with a minimum of 2 GSME Device Models from different manufacturers designed to meet SMETS2 v3.0
DIT.3	DIT shall test Communications Hubs with a minimum of 2 GSME Device Models from different manufacturers designed to meet SMETS2 v3.0 and capable of Sub-GHz HAN communications
DIT.4	DIT shall test Communications Hubs with a minimum of 2 PPMID or combined PPMID/IHD Device Models from different manufacturers designed to meet SMETS2 v3.0
DIT.5	DIT shall test Communications Hubs with a minimum of 2 PPMID or combined PPMID/IHD Device Models from different manufacturers designed to meet SMETS2 v3.0 and capable of Sub-GHz communications
DIT.6	DIT shall test Communications Hubs with a minimum of one Device Model for each of the leading ZigBee Alliance silicon stack providers
DIT.7	DCC shall select Device Models for DIT using dry-run qualification events and commercial proposals from Device Model providers to support DIT activities
DIT.8	DIT shall specifically ensure that Communications Hubs are verified as capable of complying with: • GBCS v2.0 10.6.2.6 (Frequency Agility) • GBCS v2.0 10.6.2.2 (Duty Cycle Monitoring)

DIT.9	DIT shall include risk based regression testing of Communications Hubs with a minimum of 2 SMETS2 v2.0 ESME and GSME Device Models selected to be representative of a significant proportion of the installed base of SMETS2 v2.0 Devices at the time of undertaking DIT
DIT.10	Should actual HCALCS Device Models exist and be in a suitable state of readiness, DIT shall test Communications Hubs with a minimum of 1 HCALCS Device
DIT.11	Removed
DIT.12	DIT shall test Communications Hubs with a minimum of 2 IHD Device Models from different manufacturers
DIT.13	DIT shall include end-to-end testing of the Local Command Interface using Hand Held Terminal Devices, if available, or using the DCC tool required to be developed for testing in SIT[7]
DIT.14	Removed
DIT.15	DIT shall include regression testing of SMETS2 v2.0 Devices with R2.0 of DSP

Table 9 DIT Requirements

6.5. Requirements and Focus Areas for Transition to Operations Testing

The Transition to Operations (TTO) Test Phase will include Business Acceptance, Operational Acceptance and Security related requirements as focus areas to transition R2.0 solution to operations. TTO Testing will focus upon the service management processes as SIT will have tested technical end-to-end functionality. Completion of SIT Testing is a prerequisite for TTO Test execution to start. Support from the DCC Systems Integrator and CSPs is required to carry out internal and external testing as part of TTO Testing.

The Environment Plan deliverable will highlight how TTO will utilise existing DCC environments. It is assumed that the DCC pre-production environment will not be available for Release 2.0.

Ref	Requirement
TTO.1	Transition to Operations testing shall ensure that non-functional security risks to the production environment are identified, assessed and resolved or managed, e.g. through PEN testing, work off plans and appropriate ISMS risk entries
TTO.2	TTO will include pre-production proving
TTO.3	Prioritise the resolution of known User and Service Issues evident from testing Release 2.0
TTO.4	Review impact to existing operational Services, security processes and any adverse effects

[7] The End to End process for the Local Command interface is described in 6.2 above

TTO.5	Assess information security risk and vulnerabilities
TTO.6	Prove that the system supports business/operational requirements and/or Service design
TTO.7	Transitional, business, operational processes and documents are proven and in place
TTO.8	Provide confidence that solution/services are suitable for wider infrastructure, fully implemented and fit for live service
TTO.9	TTO will test DCC internal systems and processes, including but not limited to the Cognos business information management/management information tool, SMKI Recovery and Repository Management
TTO.10	DCC operations will be included as a test participant in order to validate their processes, scenarios and procedures supporting User activity
TTO.11	Determine the potential impact of Release 2.0 on operational demand management, through regression testing and non-functional testing. Specifically this will include detailing the final message sizes

Table 10 TTO Requirements

7. Common Testing Requirements and Activities

The following sections describe the approach to testing that is required for all test phases and stages, unless explicitly described otherwise.

As a general principle, the established testing and test assurance governance, resources, processes and other activities developed by DCC for previous releases will continue – except as where explicitly required otherwise by this Testing Approach Document.

7.1. Test Activities

For each Test Phase, the following activities will be performed;

- Prepare and maintain a Test Phase Approach
- Implementation of testing infrastructure
- Test Phase planning
- Identification of test scenarios
- Design of test scripts
- Produce test specification document

- Produce requirements traceability matrix, or equivalent
- Design and preparation of test Data, including loading of test Data into the test environment
- Preparation of test execution schedule
- Execution of testing
- Performing quality gate reviews
- Test issue management
- Test issue resolution
- Release management
- Configuration management
- Test Progress reporting
- Test assurance of third party components
- Training for Test Execution

7.2. Test Method

As for previous DCC Releases, testing will be conducted using high-level test scenarios (or sequences of Service Requests for specific Test Phases). The Test Phase Approach Documents will specify the detailed testing methodologies for each individual Test Phase.

Testing should cover both functional and non-functional aspects of the dynamic interaction between solution elements, and shall provide full coverage of the DCC Service Request variables – user role, command variant, and mode of operation. Where interfaces are to be tested within a Test Phase – all relevant interfaces should be tested. Similarly, testing should account for all elements of the Modified DCC Total System, for example the internal DCC-Enterprise components that support billing and reporting.

Priority, within the design of testing for Release 2.0, shall be on the changes introduced by the scope of the Release, but also on the functionality and Service Requests that are considered to be of highest risk to Parties and Energy Consumers.

Where testing makes use of the DCC Meter Protocol Emulator, testing must include emulator configuration to provide valid data in a service response. A blank / null response cannot result in a passed test. The response must include valid data that can be successfully parsed and where relevant decrypted, to prove the response data received is as expected based on the emulator configuration for that test

DCC is seeking a significant increase in the amount of automated testing that will be performed for Release 2.0, and will require the DCC Systems Integrator to provide detail of this in the SIT Test Phase Approach Document, including reporting to demonstrate that automation expectations have been met.

Also in relation to the design of testing for SIT, coverage of DUIS v1.0 and DUIS v2.0 interfaces and how testing between regression and new elements is balanced across the interfaces and Communications Hubs types and CHTS versions.

7.3. Test Scenarios

Except for the DSP PIT test phase[8], Release 2.0 will include the non-exclusive use of test scenarios to reduce the risk of the design of testing not sufficiently matching the intended real life use of the system.

Test scenarios may, within the context of the individual Test Phases, be represented by defined sequences of Service Requests or other relevant activities.

Test scenarios shall be used in PIT to ensure that the products which are received in SIT have been exercised in an expected manner, prior to the start of SIT.

Each test phase will define test scenarios as a deliverable as appropriate, but as a minimum the definition of test scenarios will include:

- Description
- Responsibility for development
- Type (Normal, Exception, Alternative)
- Prerequisites
- Test conditions
- Verification method
- Traceability to requirements (or use case for DSP PIT)
- Test variations – User Roles, Communications Hub, mode of operation, Command variant, Device

The definition of Test Scenarios for SIT and DIT shall include and consider:

- Key common scenarios that will be experienced by the Parties in production – e.g. install and commission, Communications Hub replacement, over the air Firmware upgrade etc.
- A reasonable minimum number of exception or non-happy path scenarios
- A relevant subset of scenarios (or Service Request sequences) to reflect Network Operator Party use cases
- Include data and infrastructure security tests, taking into account DCC security architecture and security standards and patterns, alongside functional and non- functional testing

DCC will review the proposed Test Scenarios, or sequences of Service Requests, for SIT and DIT with Parties at the DCC monthly testing forum – the Testing Design and Execution Group.

Test Scenarios may be updated to take account of activities from live operation, subject to suitable change controls.

[8] DSP PIT is based on Use Cases.

Test Scenarios will also include sequences for use by DCC operations and DCC finance in order to test other DCC business processes that more generally provide support to Parties, invoice customers, and correct data errors.

Test scenarios must cover exercising all of the interfaces in DCC Systems in an end-to- end manner verifying functionality as well as data is reported correctly.

Where emulators are used, test scripts should define the required emulator configuration to provide valid data in a service response. A blank / null response cannot be considered a passed test and the response must include valid and expected data that can be successfully parsed and where relevant decrypted, to prove the response data is received as expected based on the emulator configuration to meet the defined test objective for that test.

7.4. Regression Testing

All new releases of any element of the solution from all DCC Service Providers will be subject to completing a successful regression test prior to being accepted into subsequent testing phases and environments.

The following requirements for regression testing shall apply:

- Wherever practicable, regression testing will be automated
- Regression testing will be an ongoing activity
- Any regression testing must include the SMKI – even if that element has not been changed[9]
- The regression test approach for each phase will be described in the Test Phase Approach Document
- The scope of regression, where appropriate, is permitted to be risk-based with regard for combinations of User Role, Command variant etc. The exact scope of regression shall be defined in the Test Phase Approach Document for each phase
- If risk based regression is used within a test phase, as a minimum it should include key processes
- Regression testing of the uplifted technical specifications with single band Communications Hubs cannot be risk based
- The Regression Test Pack (test scripts, test data and documentation) will be submitted to DCC at the end of the test phase, with any agreed omissions being rectified promptly.
- As part of the completion of testing phases, a minimum of two full regression cycles will be undertaken to provide confidence in the stability of the release[10]
- Regression testing for DIT must be completed against Devices for single band Communications Hubs. This requirement also applies to dual band Communications Hubs except where no suitable Device is available to test against. Only where suitable Devices are not available will it be possible to use emulators to complete DIT regression testing.
- User Regression Testing, as required by the obligations set out in this Testing Approach Document, must be completed by certain Supplier Parties.

[9] Not in scope for PIT

[10] Not in scope for DSP PIT

7.5. Dependencies and Assumptions

The following table describes the dependencies that need to be satisfied in support of Release 2.0 – individual test phases are expected to detail specific dependencies.

No.	Description	Dependent Upon
1	Commencement of specific test phases	Availability of test environments for Release 2.0
2	Commencement of UIT	Availability of the UIT-B environment, Communications Hubs and supporting User guidance
3	Commencement of DIT	Availability of Devices capable of satisfying the DIT Device Selection criteria (as outlined in 5.4 above)

Table 11 - Dependencies

In order to deliver Release 2.0 as a whole with a suitable level of confidence in the planning and assurance of the testing, there is an underlying principle that all solution elements will be fully tested and assured before being used in subsequent test phases. Therefore, SIT cannot test solution elements that have not received an approval to proceed certificate from PIT, issued by DCC – but the commencement of SIT is not dependent upon the whole scope of PIT being completed.

The following table describes the assumptions that underpin this test approach:

No.	Description
1	All solution elements will be PIT tested and gated before being subjected to SIT, i.e. defects will fall within agreed thresholds and any Work Off Plans (see Table 13) will be agreed with DCC
2	Emulators and Devices used in SIT and DIT will be assured and approved as fit for purpose prior to being used in testing

Table 12 - Assumptions

8. Deliverables

DCC will follow the testing documentation practices established for earlier releases. These are described at a high level in this section, and specific enhancements and requirements for Release 2.0 are highlighted.

8.1. By Test Phase

Deliverables will be produced for each Test Phase. The Test Phase Approach Document will detail the other deliverables required for the individual Test Phase.

For Release 2.0, a UIT Test Phase Approach Document for UIT is required. The provisions of the Enduring Test Approach Document apply, where relevant, to all testing carried out in accordance with this Testing Approach

Document modified, where necessary, to reflect the fact that the testing in this document applies to the Modified DCC Total System and includes 1.1 Communications Hubs in addition to Communications Hubs.

For the SIT and DIT Test Phase Approach Documents, DCC Test Assurance will introduce an industry review and feedback process, whereby content and/or the documents themselves will be circulated and discussed with the DCC Testing Design & Execution Group and the SEC Panel Testing Advisory Group.

The author for individual Test Phases will create the deliverable, which will be subject to the established DCC documentation review processes and 8.2 below:

- PIT – DCC Service Providers
- SIT – DCC Systems Integrator
  - OCT – Communications Service Providers
- DIT
  - DCC Test Assurance – Test Phase Approach Document, Test Scenarios
  - DCC Systems Integrator – All other DIT deliverables
- UIT – DCC Testing Services
- TTO - DCC

The table below describes the generic content and anticipated timing of the deliverables that may be required to be produced for each Test Phase by the Test Phase Approach Document.

Deliverable	Description	Timing
Test Phase Approach Documents[11]	Describes for the relevant test phase: the activities, participants, resources, roles and responsibilities, assurance requirements, reporting, success criteria and other information relating to the execution of the Test Phase. Where relevant, the Test Phase Approach Documents shall also define the entry and exit criteria, and the basis of any risk basis for regression	Following any applicable review cycle with industry, final version to be submitted to DCC by the relevant DCC Service Provider no later than 20 Working Days before the commencement of test execution. Following approval by BEIS, Test Phase Approach Documents will be published on the DCC website.
Test Plan & Test Schedule	Details the extent of the testing to be carried out and the responsibilities of DCC Service Providers and other parties	Final approved version to be provided to DCC by DCC Service Providers DCC no later than 10 Working Days before the commencement of test execution, including identification of any security constraints, e.g. sensitive scripts

[11] There will be a SIT Approach Document, a DIT Approach Document, a UIT Approach Document and a TTO Approach Document

Test Specifications	Includes Requirements Traceability Matrix and Test Scripts	To be provided to DCC by DCC Service Providers no later than 20 days before the commencement of test execution
Test Readiness Reports	Statement of readiness to commence testing	To be provided to DCC by parties undertaking testing, on a weekly basis, commencing no later than 20 days before the start of test execution
Test Results	Detail may vary by Test Phase – report content and frequency will be defined by the Test Phase Approach Document	Made available by DCC Service Providers for review DCC throughout test execution
Test Issue Log	Outstanding Testing Issues	Made available by DCC Service Providers for review by DCC throughout test execution[12]
Regression Test Pack		To be provided to DCC by DCC Service Providers with the final Test Stage Completion Report
Test Phase Completion Report	Will follow the format and content established for earlier DCC releases, and will include; • Overview of testing undertaken • Actual number of tests run, passed, failed and not run • Explanation of any tests not run • Test issue I.D. detail for failed tests • Number of test issues outstanding, split by severity • Number and severity of test issues raised • Specification of test environment used	Draft version to be provided to DCC by DCC Service Providers DCC no later than 10 working days before the planned end of test execution Final version to be provided to DCC by DCC Service Providers DCC within 5 Working Days of the completion of test execution

[12] This can be via direct access to the system, or through the provision of regular reports from the system

	- Recommendations for tests to be included in the next Test Phase - Lessons learnt during the Test Phase	
Test Scenarios	May comprise of planned and sequenced series of Service Requests.	To be available from DCC Service Providers at the same time as the finalised Test Phase Approach Document.
Work Off Plan	A plan to resolve outstanding issues	To be provided to DCC by DCC Service Providers with the final Test Stage Completion Report.

Table 13 – Deliverables

8.2. Specific Deliverables

DCC will publish the following documents.

Deliverable	Description	Timing
Environment Plan	Describes the plan for the utilisation of specific environments for each test phase, and how R2.0 will manage issues within the 1.x environments	To be provided by DCC as soon as possible following the Test Phase Approach Document being approved and prior to the start of R2.0 SIT
Environment Guide for UIT Participants	Describes the approach, policies and procedures for users testing across multiple UIT environments. Will include, as a minimum, details of Device certification and mobility, triage, defect and fix management, change management, Device management in UIT	To be provided by DCC Testing Services Team as soon as possible following the Test Phase Approach Document being approved and prior to the pre-UIT pipe-cleaning tests to be run by Users
DIT Device Selection Approach	Describes the approach for selecting the Devices to be used in DIT	To be provided by DCC Device team alongside the DIT Approach Document
Independent Assurance Reports	As described in section 16, a range of independent assurance activities will be undertaken – where appropriate there will be reports	As determined by the timing for the completion of the assurance

CTSD Update	DCC will propose changes to update CTSD to reflect the new service requests for Release 2.0, and the options for evidence for participants undertaking additive testing	DCC will consult on the updates to the CTSD following confirmation of this Testing Approach Document by the Secretary of State
Test Communications Hub Definition	Describes the capabilities and highlights the differences between the PTCH and ITCH Devices	To be presented and discussed at DCC forums (TDEG, CH Forum etc.)
PIT Communications Hub Performance Information	Provides the results of PIT testing for activities relevant to operation of Communications Hubs – e.g. firmware activation and reset timings. Will also include detail of relevant non- functional PIT testing	To be presented and discussed at DCC forums (TDEG, CH Forum etc.)

8.3. Requirements Traceability

The Service Providers will each use their own tools to manage their requirements and demonstrate traceability to both the solution design and the Pre Integration Tests. The DSP and CSPs will each provide DCC with a PIT Requirements Traceability Matrix (RTM), extracted from these separate tools.

The scope of testing will be validated by use of Test Traceability Matrix (TTM), setting out how each requirement within the scope of the direction from the Secretary of State for this release is met. The TTM supersedes the RTM developed and used within PIT.

The TTM will be prepared by DCC, based on the updates to the specifications listed in section 2.1 above, and will consider the resulting impact of those changes and resulting coexistence of enrolled Devices operating to different mixtures of versions of those specifications as well as current version of those specifications. Completion of the TTM is a dependency for SIT to commence.

The DCC Systems Integrator will support DCC in reconciling the planned Solution Testing against the TTM.

At the completion of SIT, any additional tests which have been created during SIT will be added to the TTM.

The TTM will be used by DCC, and form a key element of the independent SIT audit, to demonstrate the completion of SIT, alongside the enhanced tracking ‘Heatmap’ approach described in section 10.1 below.

9. Test Procedure

This section describes the requirements for the testing process to prove the solution for Release 2.0.

The Test Phase Approach Documents will define specific Entry and Exit Criteria for the individual Test Phases, with generic requirements for these described below.

Specific criteria for individual Test Phases, and the governance process relating to the approval of the criteria, and the evaluation of success against them.

9.1. Generic Entry and Exit Criteria

Progression through testing phases for Release 2.0 will be gated using generic and specific Entry and Exit Criteria.

The Test Phase Approach Documents will provide detail of the evidence to be gathered in the form of an evidence pack.

9.1.1 Generic Entry Criteria

The following generic Entry Criteria will gate the entry to all Test Phases:

- Test Phase Approach Document for Test Phase signed off;
- Solution Test Plan signed off (except UIT);
- Test Phase Complete Certificate for preceding Test Phase issued, unless the plan clarifies that Test Phases overlap;
- Test Specification prepared, including traceability to Requirements/Design documents (except UIT);
- Test labs, Devices, tools, stubs, environments and data are assured and accepted as fit for purpose, including external assurance;
- DCC and all relevant Service Providers have confirmed they have resources with the requisite skills and access available to support the Test Phase; and
- Approval to proceed certificate issued by DCC.

9.1.2 Generic Exit Criteria

The following generic Exit Criteria will gate the exit of all Test Phases except UIT:

- All tests run, or any exceptions documented and agreed by DCC Test Assurance Board;
- All test success criteria (e.g. test pass rate) achieved, or any exceptions documented and agreed by DCC Test Assurance Board;
- The number and severity of any outstanding Test Issues is at or below the target thresholds, or any exceptions documented and agreed by DCC Test Assurance Board;
- Test results documented and evidence captured;
- Set of test issue logs have been produced;
- Regression testing successfully completed;
- Regression test pack has been prepared or updated;
- Production of agreed Work Off Plans for any outstanding Test Issues that occurred in the Test Phase;

- Work Off Plans from preceding Test Phases have been completed; and
- Test completion reports have been produced and test completion certificates have been issued by DCC.

9.2. Governance of Test Phase Approach Documents and Entry and Exit Criteria

The following requirements shall apply in relation to each of the SIT, DIT and UIT Test Phase Approach Documents, and in particular the relevant entry and exit criteria:

(i) DCC shall prepare a draft of the document and submit the document to the SEC Panel Testing Advisory Group for comment;

(ii) Following the receipt of comments from the SEC Panel Testing Advisory Group, DCC shall update the document, taking into account the TAG comments as appropriate, and submit the draft document to the Secretary of State for approval (noting those SEC Panel comments that have not been incorporated);

(iii) DCC shall comply with any direction given by the Secretary of State to reconsider, re-consult and/or re-submit the draft document.

Where DCC proposes to deviate materially from a Test Phase Approach Document, it shall consult on its proposal to do so with the SEC Panel Testing Advisory Group and submit the proposal to the Secretary of State for approval.

DCC shall conduct its testing in a manner that is consistent with this document and the Test Phase Approach Document (as approved by the Secretary of State) for each phase including, in each case, as modified by any deviations that have been approved by the Secretary of State.

9.3. Specific Entry and Exit Criteria for Test Phases

Specific Entry and Exit criteria for individual test phases will be listed in the relevant Test Phase Approach Document.

For PIT and SIT, this will include the definition in the Test Phase Approach Document of any incremental gating into subsequent Test Phases.

9.3.1 Entry into SIT

The entry criteria for SIT shall include, inter alia:

- Completion of independent assurance of the DCC Meter Protocol Emulator will be included in the SIT entry criteria.

9.3.2 Exit from SIT

The exit criteria for SIT shall include, without limitation:

- All 1.1 Communications Hub variants introduced or changed by Release 2.0 have been tested, alongside regression testing of 1.0 CHs

9.3.3 Exit from DIT

The exit criteria for DIT shall include, without limitation:

- In the event that insufficient capable and supported Devices are available to achieve full coverage of DIT scope, DCC will complete such testing as is practical and provide detail of the reasons why DIT has not been fully completed in the Test Phase Completion report. DCC will endeavour to complete any coverage of testing with Devices in UIT should suitable Devices become available after the completion of DIT and prior to go live

9.3.4 Entry into UIT

The entry criteria for UIT shall include, inter alia:

- Successful completion of testing, assurance and DCC governance of the SIT and DIT test phases for the functionality to be promoted into UIT.

- For TSG 2.0/SBCH UIT, at least SIT and DIT regression testing with SMETS2v2 Devices will have been completed.

- For DBCH UIT, DCC will enter UIT based on the completion of SIT only.

9.3.5 Exit from UIT

The exit criteria for UIT shall include:

- Successful completion of User Regression Testing by all Supplier Parties required to carry out such testing, the details of which are defined in the UIT Approach Document. Any relaxation of the exit criteria from UIT with regard User Regression testing would be subject to approval of the SEC Panel and the Secretary of State.

9.4. Acceptance Process Following SIT Completion

Following the completion of SIT (and DIT), DCC will notify the Secretary of State, the Authority, the SEC Panel and the SEC Parties that SIT (and DIT) for a Region or Regions has ended.

DCC will provide the Authority, the SEC Panel and the Secretary of State with copies of the SIT and DIT Test Completion Report(s) and the SIT Auditor’s report, along with a list of those sections of such reports that it considers should be redacted.

DCC will review the documentation and evidence to support the relevant entry and exit criteria with the SEC Panel Testing Advisory Group to inform the SEC Panel recommendation to the Secretary of State regarding the completion of SIT (and DIT).

On direction from the SEC Panel, DCC will provide the SEC Parties and DCC Service Providers with copies of the Test Completion Report(s) and the auditor’s report, having first redacted any sections specified by the SEC Panel.

9.5. Go Live Decision and DCC Incentives

The SEC Panel and/or Parties shall provide such reasonable support and assistance that is requested from them by the Secretary of State in relation to:

(i) The Secretary of State's decision to make (or bring into legal effect) any of the SEC variations associated with Release 2,0; and/or

(ii) The administration of any Baseline Margin Project Performance Adjustment Scheme (having the meaning given to that term in the DCC Licence) relating to Release 2.0, including as set out in any BMPPA Scheme Principles (also having the meaning given to that term in the DCC Licence).

DCC will undertake a review with Parties of their activities, progress and concerns from UIT, and include collected feedback to the Secretary of State as part of the DCC go live activities.

The process for Parties to provide feedback to DCC on their UIT experiences, and how DCC will review and present the feedback will be defined in detail in the UIT Approach Document.

Supplier Parties that undertake User Regression Testing will provide the DCC with a self- certification of completion of User Regression Testing. The DCC will consider all such completed User Regression Testing as a part of the DCC go live activities.

The final report of UIT feedback and User Regression Testing will be reviewed with the SEC Panel prior to inclusion in the DCC go live submission to the Secretary of State.

DCC will provide the following materials as part of the submission to the Secretary of State relating to go live, in addition to the established DCC live services criteria:

- UIT feedback and User Regression Testing report
- UIT defect report
- All independent assurance or audit reports prepared for Release 2.0
- OCT completion reports.

9.6. Post Go Live Activities

In order to mitigate the risk to Energy Consumers, DCC will continue to offer the support for production provided at R1.3 go live, whereby for a maximum period of six months following the Release 2.0 go live date Communications Hub firmware upgrades are not initiated unless requested by the User.

This allows Users to continue to perform regression testing in Device and User System Tests (carried out in accordance with Section H14.31 of the SEC) with specific combinations of Communications Hubs and Devices and resolve issues without affecting service to Energy Consumers.

This requirement also applies to the firmware supported for the installation and commission process until a User confirms they accept that the new Communications Hub firmware operates acceptably with their Devices.

9.7. Test Phase Success Criteria

For SIT and DIT and the testing for SP UAT the following Test Success Criteria will be included in the Exit Criteria:

- 100% of tests listed in the Test Specifications have been executed, or any exceptions documented and agreed with DCC, and reported to SEC Panel;
- at least 85% of planned tests have been passed, or any exceptions documented and agreed with DCC, except for regression testing with single band Communications Hubs in DIT where 100% of tests passed is the requirement

9.8. Test Issue Defect Masks

The following table lists the standard target thresholds for outstanding test issues in each test phase.

Test Issue Severity	PIT	SIT	DIT	TTO
1	0	0	0	0
2	0	0	0	0
3	15	15	15	15
4	30	30	30	30
5	60	60	60	60

Table 14 Test Issue Thresholds

Note that:

- The defect mask thresholds are applied as part of the exit criteria for relevant test phases, and apply cumulatively if there are iterative deliveries within a test phase, for example from PIT to SIT or from SIT to UIT. For example there will never be more than 15 Severity 3 defects per Service Provider at an exit gate.
- BAT defects will be included in the TTO defect mask
- For PIT, SIT and DIT, the figures in Table 14 Test Issue Thresholds are per DCC Service Provider, i.e. 15 Severity 3s for the DSP, 15 for CSP N and 15 for CSP C/S
- The defect masks shall include any security defects within the relevant testing phase
- the Test Assurance Board, including industry representatives, may judge that the next Test Phase can start even if the target thresholds set in the Exit Criteria for the Test Phase Plan have not been achieved, provided that an agreed work off plan is in place

- If the Test Assurance Board, including industry representatives, believes that an exception for a Severity 2 issue at SIT exit should be considered, DCC will request an ex-committee review by the SEC Panel before confirming SIT exit
- A defect mask will apply for UIT Exit and will be linked to the User Regression Testing. The Exit Criteria are detailed in the UIT Approach Document.

9.9. Work Off Plans

Work off plans will be produced by each Service Provider as part of the quality gate process at the end of Testing Phases, detailing the defects that are outstanding and the plan for resolving them.

Each Service Provider must resolve all of the items within the work off plan within the following timescales;

- For Severity 3 defects, within 20 Working Days from the quality gate meeting
- For Severity 4 defects, within 40 Working Days from the quality gate meeting
- For Severity 5 defects, within 60 Working Days from the quality gate meeting

In the event that the timescales for the work off plan are not met, the DCC Service Provider shall produce and agree a correction plan with DCC.

If a Test Phase Complete Certificate has been issued subject to completion of a work off plan, and the work off plan has not been completed within the applicable time period, then DCC will revoke the Test Phase Complete Certificate unless the failure relates solely to Severity 5 test issues.

9.10. UIT Test Issue Thresholds and Work off Targets

During the UIT Test Phase, by DCC Service Provider, the following performance targets will apply to defects assigned to a Service Provider for resolution, at any given point:

- 0 Severity 1 defects
- Fewer than 5 Severity 2 defects
- Fewer than 15 Severity 3 defects
- Fewer than 30 total Severity 4 and 5 defects

In all cases, each DCC Service Provider must resolve UIT defects within the work off timings shown below, measured from the point of the defect being accepted by the Service Provider:

- For Severity 1 defects, within 10 days
- For Severity 2 defects, within 20 days
- For Severity 3 defects, within 40 days
- For Severity 4 defects, within 50 days

The above targets and work off times shall apply to defects associated with UIT testing of the new R2 functionality in relation to both Single and Dual Band.

Defects associated with User Regression Testing are subject to the UIT Exit Criteria described in the UIT Approach Document.

10. Test Result Management & Reporting

Test Result Management and Reporting is to be provided to DCC by the DCC Systems Integrator with input from SPs for PIT, SIT, UIT, DIT and TTO Test phases, as relevant, on a frequency to be detailed in the Test Phase Approach Documents.

10.1. Tracking & Reporting

HP's Application Lifecycle Management (ALM) Test Management tool will be used to manage testing and testing issues[13].

All requirements, scripts, tests, execution results and defects are to be maintained in ALM. Connectivity between requirements, tests and defects is to be maintained for traceability and reporting purposes.

Overall responsibility of maintaining traceability of test and defects will lie with the DCC Systems Integrator for SIT Test Phase.

DCC Systems Integrator shall implement a tool and processes based upon the existing solution revised with learnings from previous releases to provide enhanced visibility and reporting of the progress, completion and coverage of testing for SIT across a number of parameters.

Security testing defects should be recorded/reported with other testing defects, redacted as required, but counting towards defect masks.

10.2. Weekly DCC Test Execution Report

DCC will provide a weekly Test Execution report to the SEC Panel and the Secretary of State. The content of this report will reflect the status of progress within Release 2.0, based upon data from HP ALM and other DCC Systems.

It will include detail of testing progress in relevant test phases, reporting on testing issues and matters relating to the capacity and availability of the user testing services. Whilst SIT, DIT and TTO are being conducted, it will include detail of the progress against the testing glide path. The report will include testing coverage of functional areas, alongside Service Requests. The content of this report will be anonymised and redacted as if it was subject to Section H14.44 of the SEC.

10.3. SIT & DIT Test Completion Reports

In accordance with 9.3.1 above, DCC will produce its own Test Completion Reports when it considers that the Exit Criteria required by the SIT/DIT Test Phase Approach Documents for a Region have been met. The report will provide evidence of the testing undertaken, the results of testing and how the exit criteria have been met.

DCC will also produce a TTO Test Completion Report.

[13] Except where not applicable for PIT

These reports, alongside any relevant independent assurance reports, will be provided to the Authority, the SEC Panel and the Secretary of State.

11. Acceptance and Test Assurance

DCC has established processes for the acceptance of testing activity completion – these will continue for Release 2.0. The DCC Test Assurance Board will conduct quality gate meetings and review testing completion reports before issuing Test Completion and Approval to Proceed Certificates.

Where a Test Completion Certificate has been issued subject to completion of a Work Off Plan, and the Work Off Plan has not been completed within the applicable time period, then the Test Completion Certificate will be revoked unless the failure relates solely to Severity 5 test issues.

11.1. DCC Service Provider Self Assurance

DCC Service Providers will continue to assure their own PIT activities against this Testing Approach Document and specific PIT Test Phase and Test Plan. Service Providers will also continue to make their relevant testing deliverables available to the other Service Providers and exchange constructive comments to ensure solution and testing compatibility.

11.2. Test Assurance by DCC

DCC will continue to assure Service Provider testing using the processes and activities established for earlier releases, and will include the following methods, at times determined by the individual Test Phase Approach Documents:

- Test Assurance Board quality gates
- Test Witnessing
- Test Observation
- Reviewing Test Evidence
- Test Quality Audits
- Product Inspections
- Document Review

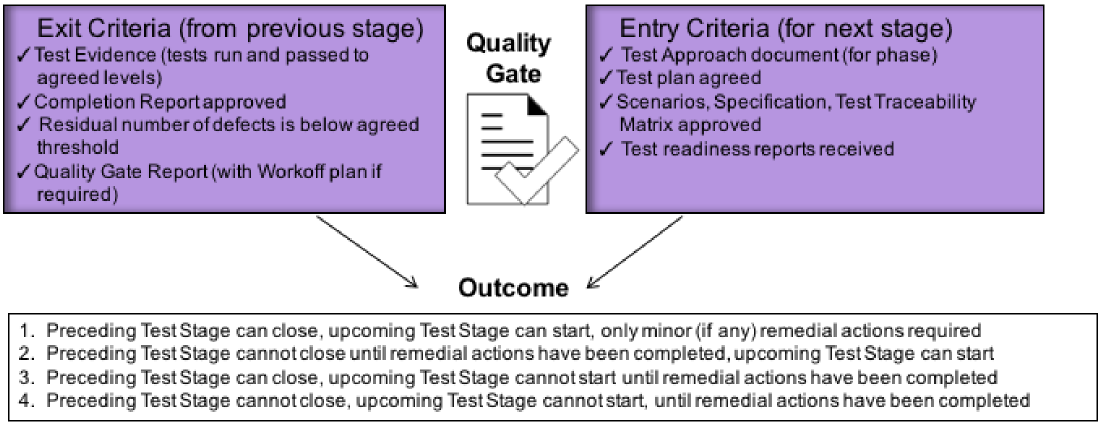
11.2.1 Quality Gating & the DCC Test Assurance Board

DCC will continue to operate the Quality Gating process developed for Release 1.x and enhanced through experience.

The Quality Gate process provides:

- Controlled entry of functionality into subsequent test phases
- Formal and objective evidence that test criteria have been met for a stage

- Transparency of test activities and outcomes to facilitate DCC Test Assurance
- Formal evidence for signoff of Service Provider test milestones and/or associated payments
- A mechanism for managing remedial work associated with closure of test stages


Exit Criteria (from previous stage)
Quality Gate
Entry Criteria (for next stage)
Outcome

Exit Criteria (from previous stage)

- ✓ Test Evidence (tests run and passed to agreed levels)
- ✓ Completion Report approved
- ✓ Residual number of defects is below agreed threshold
- ✓ Quality Gate Report (with Workoff plan if required)

Entry Criteria (for next stage)

- ✓ Test Approach document (for phase)
- ✓ Test plan agreed
- ✓ Scenarios, Specification, Test Traceability Matrix approved
- ✓ Test readiness reports received

Outcome

1. Preceding Test Stage can close, upcoming Test Stage can start, only minor (if any) remedial actions required
2. Preceding Test Stage cannot close until remedial actions have been completed, upcoming Test Stage can start
3. Preceding Test Stage can close, upcoming Test Stage cannot start until remedial actions have been completed
4. Preceding Test Stage cannot close, upcoming Test Stage cannot start, until remedial actions have been completed

Figure 2 – DCC Quality Gate Process

The Quality Gate process will apply to all PIT and SIT testing, and relevant elements of UIT, DIT and TTO testing.

The Quality Gates from PIT into SIT and from SIT into UIT are operated as DCC Test Assurance Board gates.

The Test Assurance Board (TAB), is a meeting called, facilitated and chaired by the DCC Head of Test Assurance, attended by Service Providers, the DCC Systems Integrator, relevant attendees from DCC departments and nominated representatives of the industry, on behalf of the BEIS Smart Meter Delivery Group.

11.2.2 Test Witnessing

DCC will agree, in advance, with the SPs which tests it wants to witness during FAT and Service Provider UAT. Details of these tests (which will be a subset of System Tests for FAT and a subset of Solution Tests for UAT) will be described in the FAT and Service Provider UAT test plans. The SPs will provide DCC with a schedule of when the tests will be executed and invite DCC to either witness on-site or remotely. The witness will have the skills required to fulfil the role. The SP will provide the witness with relevant documentation and access.

For R2.0 DCC Test Assurance and the SIT Auditor must be given full access to attend and witness such testing.

Execution of the agreed set of tests will be performed by the relevant SP test analyst, and there will be:

- No deviation from the scripts (e.g. in response to “what if” questions raised by witnesses)
- No hands-on execution by witnesses

Test issues raised during witnessing will be entered in to the relevant Test Issue Management tool and progressed through the Test Issue Management process.

As far as possible, any queries and issues arising during the witnessing period will be addressed at the time with the relevant SMEs. A wash-up session will be convened at the end of the witnessing period to discuss the outcome of witnessing and to agree any outstanding queries and issues.

DCC may elect to receive System/Solution Test execution evidence as a substitute for some tests nominated for witnessing.

11.2.3 Test Observation

By prior agreement with the SPs on the timing, duration and scope, DCC staff may observe test execution and test issue management activities during System Testing and Solution Testing in order to familiarise themselves with SP processes and the systems under test. The DCC observers will have the skills required to fulfil the role.

12. Testing Issue Management

This section describes the processes for Testing Issue Management and the Test Issue Lifecycle. The Testing Issue Management process remains the same across all phases of testing in scope[14] with a slight variance to how UIT (i.e. UEPT and End to End testing) Testing Issues are handled.

The process defined in the Testing Issues Resolution Process covers both SIT and UIT based testing. However there are small variations that arise due to the requirement to interact with Service User Testing Participants. In summary the main differences are as follows:

Triage process: This varies depending upon the types of Testing Issue detected, particularly where the issue is CSP related (where test labs are used) rather than DSP related.

Communications process: In UIT Testing Participants may or may not have access to the Testing Tool used for Testing Issue recording, in which case a manual workaround process is employed.

Escalation: Where a Testing Issue needs to be referred to the Issue Resolution Board (IRB) and a Service User is the Testing Participant that is the subject of the IRB, special information disclosure conditions will apply.

For clarity, Testing Issue Management will not apply to TTO.

The 'Testing Issue Resolution Process' document can be found on the DCC website: *https://www.smartdcc.co.uk/media/332365/testing_issue_resolution_process.pdf*.

This document will be updated by DCC to incorporate the option for Testing Participants to use Instrumented Test Communications Hubs in their own Remote Testing Laboratories.

12.1. Logging and Triage of Test Issues

Where testing is taking place in the SIT environment all issues relating to the DCC solution will be logged and recorded in HP ALM by the person executing the test. New testing issues will be referred to the Triage team, who will:

- classify them as one of:

[14] The test issue management process does not apply to DSP PIT, which will follow the existing DSP PIT defect management process

(i) Testing issue:

- that prevents execution of a test; or
- that causes an unexplained or unexpected outcome or response to a test

(ii) not a Testing issue (e.g. a misunderstanding)

(iii) duplicate of an existing Testing Issue

(iv) change to DCC systems i.e. not a valid Testing issue

(v) a situation where more information is needed

- set their Severity and Priority (see Section 12.7 for definitions)
- evaluate the potential impact on the DCC production solution, and record that evaluation in a suitable, searchable field on HP ALM, or other appropriate tool
- assign the Testing Issue to the relevant Resolver Group (typically a DCC Service Provider)

In situations where a Testing Participant wishes to raise a Testing Issue whilst undertaking testing in the UIT environment (for example during UEPT), then the above process applies with the following variations:

- The Testing Participant may have access to the DCC hosted HP ALM system, in which case they may log the Testing Issue themselves via their web browser. If they don’t have this capability then they are required to log the Testing Issue using a manual spreadsheet form (full documentation is available on the DCC website), which is then picked up and logged in HP ALM by DCC on their behalf.
- Classification, setting Severity/Priority and assignment to Resolver Groups is carried out in the same way as described for issues raised in the SIT environment above.
- The process of logging and triage for testing in UIT testing may involve more steps than are required for SIT, due to the remote nature of some of the testing, specifically where testing occurs in remote test labs without an Instrumented Test Communications Hub. In such cases it may be necessary to rerun the tests that cause the Testing Issue so that additional diagnostic information can be captured, for example Communication Hub logs, prior to the assignment of the Testing Issue for triage. Further documentation defining this process has been prepared by DCC and is available to Testing Participants on request.
- Testing Participants may log Testing Issues discovered in UIT for further assessment and triage, even where they are discovered during testing that hasn’t followed a specific test script.

12.2. Resolution of Test Issues

The DCC Systems Integrator Testing Issue Manager will:

(i) regularly review all outstanding test issues to ensure that they are resolved with reasonable speed

(ii) agree with the relevant SP Test Managers the defect fixes to be included in each Release to the SIT environment

(iii) report progress directly to stakeholders.

12.3. Target Response Times

For issues raised in SIT, DIT and UIT, the following table lists the target response times, which apply and are measured from the point at which the issue is logged in the test issue management tool.

The timings:

- Are in working hours
- Assume the working day to be Monday to Friday, 08:00 to 18:00
- Assume that a suitable Triage group and Issue Resolution Board are each available to meet once a day
- Are for in-house supported system elements only: system elements supported by third parties are subject to the timings defined in the relevant contracts
- May need to be adjusted for cases where a resolver group is not working to UK time.

Note that the targets are not binding, and there are no penalties associated with non- achievement. Target response times are subject to ongoing reporting and may be reviewed to reflect circumstances in test phases.

Priority	Initial Response Completed	Triage Completed	Assessed by Resolver Group	Fix Time Assessed
1	1 hour	4 hours	6 hours	18 hours
2	1 hour	Next Triage Panel	Next Triage Panel + 2 hours	Next Triage Panel + 14 hours
3	4 hours	Next Triage Panel	Next Triage Panel + 4 hours	Next Triage Panel +22 hours
4	4 hours	Next Triage Panel	Next Triage Panel + 6 hours	Next Triage Panel + 30 hours

Table 15 Target Issue Response Times

The Triage Panel will meet daily.

The checkpoints in the above table are defined as follows:

- Initial response completed: acknowledgement sent to the person raising the Testing Issues
- Triage Completed: the Triage Panel (either scheduled or emergency) has triaged the test issue and either a) assigned it to a resolver group, or b) escalated it to the Issue Resolution Board
- Assessed by Resolver Group: the resolver group has either accepted or rejected the test issue

- Fix Time Assessed: the resolver group has estimated how much effort it will take the fix the test issue.

Note also that there are not target fix times because:

- In a complex, bespoke system such as the DCC Total System, there will be an extensive variation in fix times
- Any such targets would be inconsistent with the existing DCC Service Provider Contracts.

12.4. Assurance and Disputes

12.4.1 Assurance

The Triage Panel, comprising each DCC SP's design authorities, the DCC System Integrator and the DCC including DCC Design Authority, and chaired by the DCC Systems Integrator Triage Manager, will meet daily (and on demand for urgent test issues which are delaying testing) to:

- resolve cases where the ownership of a test issue is disputed;
- confirm, by a process of review of all new issues, that test issues are being given the correct Severity and Priority by the local triage process or Service User raising the test issue;
- confirm, by a process of sampling, that Priority 1 and 2 defects are being resolved at the requisite speed.
- The DCC's Issue Management Team are responsible for reviewing by sampling the execution of issue management activity and for ensuring that all aspects of this are correctly undertaken and documented, including (but not limited to):

(i) Full and proper adherence to the process;

(ii) Use of appropriate and sufficient communications around the process;

(iii) Documentation of the process having been properly followed via commentary, collection of appropriate support documentation, e.g. logs, evidence and release notes;

(iv) That each action that has been taken within the process has been taken by the appropriate member of staff; and

(v) That audit requirements have been met.

12.4.2 DCC Issue Resolution Board

Testing Issues can be referred to the DCC Issue Resolution Board (IRB) as a means of escalation in the following circumstances:

(a) Agreement cannot be reached on the severity level and priority status of the Testing Issue;

(b) Agreement cannot be reached on the status of a Testing Issue; or

(c) The Testing Participant is dissatisfied with the speed at which the Testing Issue is being resolved; or

(d) A Testing Participant disagrees with the manner in which a Testing Issue should be resolved.

In the case of a), b) or c), the Testing Participant (or DCC Service Provider) must provide justification for its view and DCC may request further supporting information from them.

The IRB will determine:

(a) The severity, priority, status and response timescale that should apply to the Testing Issue;

(b) The organisation responsible for rectifying the Testing Issue;

(c) Whether the error is due to an issue with the design baseline, which could result in a Change Request (in which case the matter will be referred to the DCC Design & Assurance Director); and

(d) Whether the Testing Issue should be rectified pre-DCC Live or postponed to the post- DCC Live release.

The IRB is scheduled to occur every working day by default, and will be cancelled if not required.

Where a Testing Participant disagrees with the determination of the IRB they may request that DCC refers the matter to the SEC Panel, as if Section H14.43 applied. Note that this is only available where a Testing Participant disagrees with the manner in which a Testing Issue should be resolved.

12.5. Reporting of Test Issues

Information on the status of test issues will be reported by the DCC Systems Integrator to DCC in the weekly Test Execution reports described in 10.2 above.

DCC will report information regarding Testing Issues that have the potential to impact testing undertaken by Testing Participants during End to End Testing.

12.6. Test Issue Management Process

The detailed Test Issue Management process will be reviewed and revised in conjunction with the creation of the Release Test Plan.

The high level lifecycle for test issues raised during testing is shown in the following diagram.

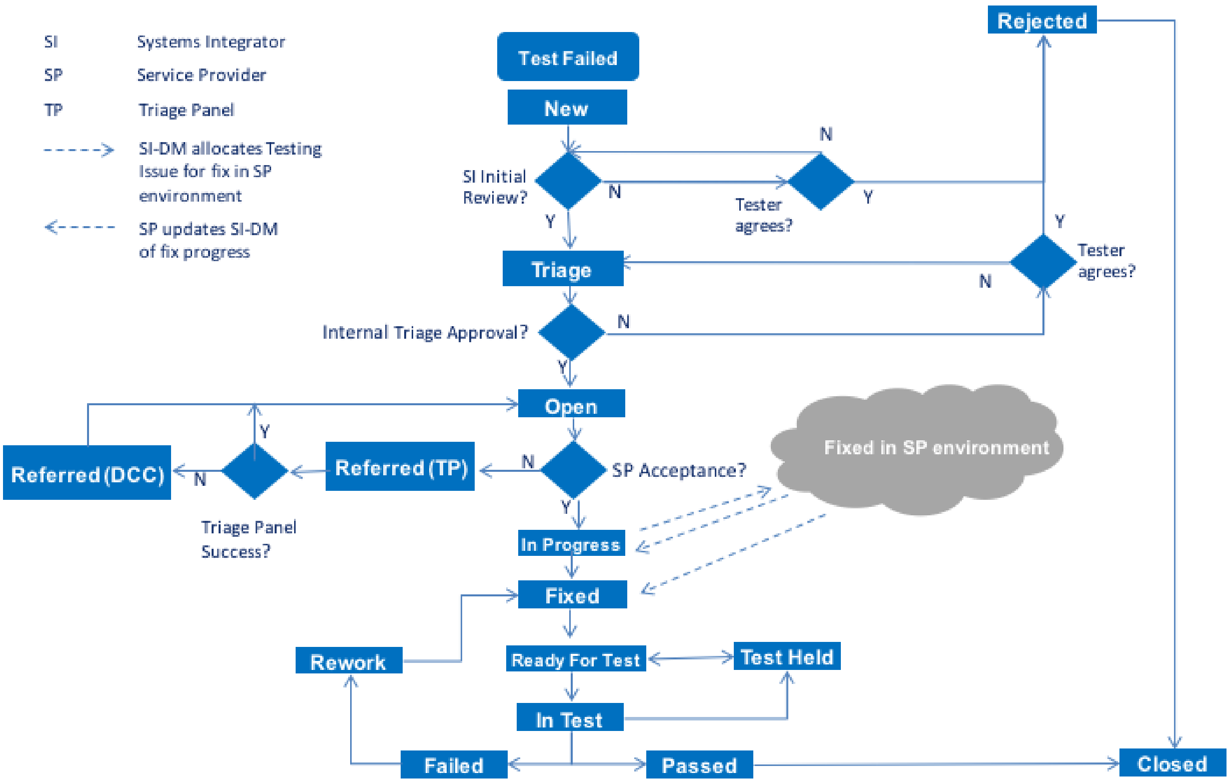


Figure 3 – Test Issue Lifecycle (with transition states)

Note that test issues can be passed back to "Triage" from the various process steps (e.g. "Failed PIT"), but these links are not shown on the diagram in order to preserve clarity.

Test Issues which are agreed to be a Change will follow the DCC Change Control process (set out in the "Core SP Change Management Process" document).

Testing Issues Resolution Process will apply for this release, which is available at the following link:

https://www.smartenergycodecompany.co.uk/docs/default-source/sec- documents/guidance/decc-guidance---testing-issue-resolution-process.pdf?sfvrsn=4

DCC will have the final judgement on the severity of a particular defect based on the impact on User operations.

12.7. Test Issue Severities and Priorities

The following table lists the standard Test Issue Severities. The Severity of a Testing Issue relates to the impact it would have on **Users and Parties, and/or DCC,** if released into production. Particular consideration should be taken of the impact on end consumers, especially those in vulnerable circumstances.

Issue Severity	Description
1	A Test Issue which: • Prevents a User or large group of Parties from using the DCC Systems; • Has a critical adverse impact on the activities of Users and Parties, and/or DCC; • Could cause significant financial loss and/or disruption to the DCC services or

	DCC Parties; or • Results in any material loss or corruption of data. Non-exhaustive examples: • An issue leading to non-availability of the DCC Services; • An issue leading to non-availability of the CSP core solution element(s).
2	A Test Issue which: • Has a major (but not critical) adverse impact on the activities of Users and Parties, and/or DCC but the service is still working at a reduced capacity; or • Causes limited financial loss and/or disruption to Users and Parties, and/or DCC Non-exhaustive examples: • An issue leading to non-availability of the network management centre; • An issue leading to loss of resilience of the SM WAN gateway; • Large areas of functionality will not be able to be tested.
3	A Test Issue which: • Has a major adverse impact on the activities of Users and Parties, and/or DCC but which can be reduced to a moderate adverse impact through a work around; or • Has a moderate adverse impact on the activities of Users and Parties, and/or DCC.
4	A Test Issue which: • Has a minor adverse impact on the activities of Users and Parties, and/or DCC Non-exhaustive examples: • Minor service interruptions in the business process or functionality of the DCC Systems and/or Services
5	A Test Issue which: • Has minimal impact to the activities of Users and Parties, and/or DCC Non-exhaustive examples: • Trivial issues with workarounds which are noted for future releases but minimal impact of running existing services

Table 16 Test Issue Severities

The following table lists the standard Test Issue Priorities. The priority of a Test Issue is the impact of the issue on **testing** progress – it is a measure of how quickly the issue needs to be fixed to allow development and testing to continue.

Issue Priority	Description
1 – Urgent	Has a severe impact on testing. Must be fixed immediately. A critical set of functionality scoped to be tested cannot be completed and needs this issue fixed before testing can continue.

2 – High	Has a major impact on testing. Should be fixed within a day of the issue being logged. A major set of functionality can only be tested by use of a complicated workaround which is slowing down test progress.
3 – Medium	Has a medium impact on testing. The issue could be fixed before release of the current version is in development. Incident affects pass success on some tests but the issue can be by-passed for other tests by means of a simple workaround.
4 – Low	Has a minor impact on testing. The issue would be fixed if there is time, but it could be deferred until another build release. The issue is normally cosmetic in nature and does not affect the key delivery of the business requirements

Table 17 Test Issue Priorities

13. Test Resources

Given the scale of Release 2.0, and the number of organisations supporting its delivery, this document will not provide detail of the DCC internal teams or the DCC Service Providers who will be undertaking the actual testing, but does provide detail of the DCC Test Assurance Team who are responsible for assuring compliance with this Testing Approach Document.

The Test Phase Approach Documents will also highlight how Release 2.0 will impact Release 1.0 resources.

This section also describes the Testing Stubs which will be used, and the other Testing Tools.

13.1. Test Assurance Team

Notwithstanding any organisational change at DCC affecting the structure of the team, dedicated DCC resources will support the assurance of testing described in this document.

The functions and services delivered by the DCC Test Assurance Team shall include:

(a) Systems Test Assurance – responsible for assuring the progress of testing, including witnessing and observing testing within PIT, DIT,SIT and TTO; reviewing test plans, scripts and scenarios; undertaking User Acceptance Testing; providing evidence and documents into the Test Assurance Board meetings; assuring reporting by Service Providers. This team also includes the Business Acceptance Testing and Operational Acceptance Testing resources

(b) Issue Management – responsible for operating the issue management process; including chairing the Issue Resolution Board and reporting on issues for all test phases except PIT. Responsible for producing reports on testing issues, including providing regular reporting to DCC problem management on issues potentially affecting the DCC production solution

(c) Device Management – responsible for the use of Devices in DIT and UIT; maintaining GFI Testing and the Meter Protocol Emulator; providing Device expert support to triage and issue management processes; planning and managing ongoing DCC interoperability testing events; reporting on Device testing

(d) Test Assurance Management – responsible for reporting progress to industry; point of escalation for testing participants; conducting Test Assurance Board meetings; managing independent audit and assurance providers; maintaining this approach document; submitting evidence and reporting to SEC Panel and the Secretary of State as required

(e) Industry Test Team – responsible for supporting the SREPT and UEPT entry process activities; supporting user testing and managing relationships with testing participants; reporting on user testing

13.2. Test Stubs

This Testing Approach Document allows for the use of Testing Stubs where appropriate across each of the testing phases to support entry into and completion of those phases. Individual Service Providers, DCC and Testing Participants may utilise Testing Stubs to simulate or emulate elements of the solution which are either not available or practical for use in the relevant test phase. For example, within SIT, a Service User Simulator will be used to act in the role of a DCC User.

DCC has developed a Meter Protocol Emulator, capable of acting as an Electricity or Gas meter, or as a PPMID or HCALCS Device. This emulator will be used as part of SIT for Release 2.0, be used for User Entry Process Testing and made available to Testing Participants in the DCC Labs should they choose to use it in UIT.

The DCC Meter Protocol Emulator will not be used by Service Providers in PIT, they are responsible for meeting their own emulator requirements during PIT.

The Meter Protocol Emulator will be updated to enable its use to complete testing for Release 2.0 including the addition of acting as an In Home Display, and will be subject to an independent assurance activity.

13.3. Testing Tools

13.3.1 ALM

HP's Application Life Management (ALM) Test Management tool will be used to manage testing and test issues in all phases after PIT, where test management is supported by the DCC Systems Integrator.

HP ALM will be used to maintain:

- Requirements connecting to Test Scenarios/ Scripts and defects for traceability and reporting purposes across respective test phases.
- The test scripts
- Execution details of each test script (e.g. when run, by whom)
- Evidence of system behaviour (e.g. screen shot, log file) observed during execution
- The result of execution (pass, fail)
- Defects raised for failed tests (which will be linked to the failed tests).

13.3.2 GFI Testing Service

DCC shall make available an enhanced GFI testing service, being the testing service referred to in X9.1 of the SEC, enhanced to enable eligible persons to test the interoperability of Devices (other than those comprising

Communications Hubs) with the Modified DCC systems and with v1.1 CHs, such that those Devices are able to respond to Commands received from or via DCC in accordance with the requirements defined in the GB Companion Specification version 3.0. This testing service shall be made available on the same basis as Testing Services under Section H14 (Testing Services), but subject to this Testing Approach Document. This service and the requisite Test Communications Hubs must be made available by DCC by the commencement of SIT (see Section 16 – Interoperability Testing Events for further detail of this Testing Service).

13.3.3 Communications Hubs for Testing

Release 2.0 requires that DCC makes the following Dual Band Test Communications Hub variants available for participants to request for use in the UIT environment in both the DCC and remote test labs, alongside non-instrumented Communications Hubs:

(a) Prototype Test Communications Hub (PTCH) – this variant will be available to request for use in UIT, at DCC Test and Remote Test Labs if required, prior to the completion of SIT. This variant will enable participants to assure HAN connection and interoperability with other Devices, but may not support testing of all 1.1 Communications Hub functionality

(b) Instrumented Test Communications Hub (ITCH) – this variant will be available to request for use in UIT, at DCC and Remote Test Labs. It will allow participants to diagnose and assure HAN performance and interoperability with other Devices, and undertake functional testing. The ITCH shall be capable of producing logs in a format that can be easily interrogated.

A Deliverable explaining the capabilities of PTCH and ITCH will be produced by DCC.

The ITCH for Dual Band will not replace the ITCH for Single Band CHs.

13.4. Test Laboratories

Each CSP will provide a test lab facility and supporting services to enable Parties to complete User Entry Process Testing using the DCC Meter Protocol Emulator, DCC meters and DCC Communications Hubs, alongside enabling Parties to test with their own Devices and DCC Communications Hubs and SM WAN infrastructure in the User Integration Testing environment.

DCC will continue to support the use of remote test labs by Testing Participants.

13.5. Assurance of Emulators and Tools

As described in section 17.4 below, and with SEC Panel Testing Advisory Group oversight, DCC will appoint independent parties to undertake assurance of any changes to the DCC Meter Protocol Emulator and the GFI tool. The assurance activities will include the provision of a report to DCC.

- In particular, the assurance will review the ability of the DCC Meter Protocol Emulator and GFI tool to support testing and assurance of GBCS v2.0 10.6.2.6 and 10.6.2.2.

- Completion of the independent assurance will be a pre-requisite for entry into SIT

14. Roles and Responsibilities

All parties involved in Release 2.0 testing shall:

- Follow the SEC definition for “Good Industry Practice”, i.e. the exercise of that degree of skill, diligence, prudence and foresight which would reasonably and ordinarily be expected from a skilled and experienced person engaged in a similar type of undertaking as that party under the same or similar circumstances

- Take all reasonable steps to facilitate achievement of the testing objectives

- Ensure that all testing issues are evaluated for the potential impact on the DCC production solution, at the point of raising the issue or during triage, and recorded as such on HP ALM

14.1. DCC Systems Integrator

DCC shall ensure that the DCC Systems Integrator will manage SIT and be responsible for the following activities:

(a) Assure Service Provider PIT by supporting DCC, where required for:

(i) Reviewing the SP PIT Approach documents;

(ii) Reviewing the SP System Test Plan and FAT plan;

(iii) Reviewing SP Requirements Traceability Matrix;

(iv) Reviewing SP FAT test scenarios and data

(v) Reviewing SP Test Completion Reports and Work Off Plans for Systems Test and FAT for PIT; and

(vi) Attending the SP Quality Gate Review.

(b) Producing and maintaining the SIT Approach, the Solution Test Plan and the SP UAT Test Plan;

Ensuring that SIT activities are carried out in accordance with the SIT Approach, the Solution Test Plan and the SP UAT Test Plan;

Overall planning and control of SIT, including chairing entry Quality Gates between FAT and Solution Test, and between Solution Test and User Interface Testing

Maintaining Risk, Assumption, Issue and Dependency Logs for SIT

Leading the design and creation of test scenarios, test scripts, test data and test environments for SIT

Preparing test execution and environment usage schedules for SIT

Supporting the other SPs in their assigned test preparation and execution activities within SIT

Managing test issue resolution, and supporting SPs in the resolution process for selective test phases

Producing the Test Stage Plans, Test Specifications, Test Traceability Matrices, Progress Reports and Test Completion Reports for SIT and DIT

Operating the master Configuration Management Plan

Operating the master Release Schedule

Operating the Environment Plan Support the Interoperability Test Events

14.2. DCC Service Providers

DCC shall ensure that the DCC Service Providers (including DCC in its role as provider of Enterprise Systems) shall:

(a) Manage its own PIT Test Phase, including their own processes, staff, test environments, test data, test tools including emulators and test labs. Other Service Provider PIT responsibilities include:

- Provide PIT Test Approach and PIT Test Plan documents to DCC ahead of test execution;
- Provide regular progress reports on testing and testing issues;
- Provide a Test Completion Report at the end of PIT, or an equivalent report for incremental gates throughout PIT;
- Support DCC in assuring, through witnessing and the review of evidence, the quality of PIT;

(b) Support the DCC Systems Integrator in:

- Planning and control of test phases;
- Design and creation of test scenarios, test scripts, test data and test environments;
- Preparing test execution and environment usage schedules;
- Diagnosing test issues;
- Producing Test Plans, Test Specifications, Requirements Traceability Matrices, Progress Reports and Test Completion Reports;
- Contributing to the Master Configuration Plan;
- Contributing to the master Release Schedule;
- Contributing to the Environment Plan;

Establish, maintain and control their own test environments, in terms of software/hardware configuration and access control;

For tests within their agreed test boundary, under the direction of the DCC Systems Integrator;

- Execute and monitor test scripts;
- Capture evidence;
- Report progress;

Resolve test issues for their solution elements and undertake PIT testing (including regression testing) of any fixes required

Support the interoperability test events

The CSPs will:

(a) Establish, maintain and control their own Test Labs;

(b) Procure and install 1.1 Communications Hubs in their Test Labs;

(c) Install, maintain and support DCC Device Emulators in their Test Labs;

(d) In conjunction with their Communications Hub manufacturers, obtain Communications Hub certifications from the relevant authorities.

14.3. DCC

DCC shall:

(a) Comply with its obligations under this Testing Approach Document (this document);

Ensure that activities attributed to Service Providers that are described in this document are undertaken;

Use its reasonable endeavours to ensure that SIT and DIT are completed as soon as is reasonably practicable to do so;

Enter into agreements with Device manufacturers to provide and support Devices for use in DIT, following appropriate qualification or selection activity;

Support the DCC Systems Integrator in the planning, control and operation of testing;

Assure planning, preparation and execution activities undertaken by the DCC Systems Integrator and Service Providers as detailed in this document and through the Test Traceability Matrix;

Operate and Chair the DCC Test Assurance Board process to review and approve the relevant Test Documents and issue the Approval to Proceed certificates, including the approval of test phase Completion Reports;

Operate and Chair the DCC Design Assurance Board; Participate in Quality Gate Reviews;

Agree with the DCC Systems Integrator and Service providers the subsets of Solution Tests to be witnessed in the UAT stage;

Witness the execution of UAT;

Specify, procure, provide and maintain the DCC Meter Protocol Emulator Devices and Service; and

Appoint and manage the independent audit and assurance activities described in this document.

15. Environments

Release 2.0 requires the following changes to the integrated DCC environments:

- an additional UIT environment – UITb for R2.0, with the existing UIT environment becoming UITa to mirror production

- an additional SIT environment for the Central & South Communications Service Provider

These additional environments will be available as required by the overall plan for Release 2.0. Specific deliverables relating to the management and use of environments, particularly co-existing UIT environments, will be published by DCC. This will clarify the approaches to issue and Device management, triage across environments, code streams and management.

Each DCC Service Provider is responsible for establishing, maintaining and controlling its own Test Environments. Service Providers are also required to design, develop and support Test Stubs, Test Data, Test Labs and necessary hardware installations (Communication Hubs/Smart Meters/Other Devices) that are required for execution of respective test phases.

DCC Service Providers are also expected to follow necessary software installation versions, firmware versions and adhere to ZigBee and other relevant certificates.

15.1. Code Management

DCC will operate a process to merge code changes and fixes from production into the SITB environment used by R2.0. The SIT Approach Document will provide detail of the frequency of the operation of this process.

16. Device Interoperability Testing Events

DCC will continue to host interoperability testing events, with a minimum of four taking place in a twelve month period.

These events will see the CSPs provide resources and communications hub hardware to enable other participants to test their Devices with.

The aim of the interoperability events are to provide a testing environment where Device manufactures can test with the Communications Hubs in an informal yet structured way. The events are generally scheduled to test features before they reach SIT, in order to provide an element of risk mitigation.

The Interoperability Testing Events will support Release 2.0 by acting as Market Facilitation Events – allowing participants to test interoperability with Sub GHz HAN Devices.

DCC will continue to provide notice of, and reporting, following these events.

To support these events the Communications Service Providers will provide ZigBee Sub GHz Test Devices, compliant with the relevant technical specifications.

17. Audit and Independent Assurance

As part of the testing approach for Release 2.0 further assurance of the testing and the tools used will be subject to independent review.

17.1. Independent Audit of SIT Exit Criteria

DCC shall appoint an auditor (that is sufficiently independent of Parties) to monitor SIT activities and to confirm that the exit criteria have been met for each Region.

This appointment will take place a minimum of one month prior to the commencement of SIT using the existing DCC Audit and Assurance Framework Agreement.

DCC shall engage with the SEC Panel Testing Advisory Group to seek a minimum of one representative to participate in the definition of the audit scope, and the selection of the SIT auditor.

The auditor will be procured against the scope that is set out below and tender responses assessed by DCC against criteria that will include:

(a) Independence from DCC and the DCC Service Providers;

(b) Proposed Audit Approach;

(c) Relevant Experience; and

(d) Cost

The identity of the SIT auditor will be provided to the Authority, SEC Panel and Secretary of State following contract award.

17.2. SIT Audit Scope

The SIT audit will encompass activities that are undertaken in the Solution Test and SP UAT testing stages, and will provide confirmation that all exit criteria have been met including that:

- Testing had been conducted in accordance with this approach document;
- The coverage and completeness of testing, making specific reference to the Test Traceability Matrix, and the operation of the heatmap test management tool by the SI;
- A robust issue/defect resolution process has been used, including the manner in which issues have been closed, and that no bias has been introduced into the process.

The SIT Auditor will be engaged and will monitor the matters being tested pursuant to SIT during Release R2.0 and confirm that the exit criteria have been met for each Region.

17.3. Approach to SIT Audit

The SIT audit will be undertaken on a Region by Region basis.

The auditor will be required to produce an audit approach document for review by DCC prior to commencement of the work. A risk-based approach will be taken to the audit and the manner in which the risk assessment will be conducted should be set out in the audit approach document.

The audit will include: observation of test activities during Solution Test and witnessing during SP UAT; review of test artefacts; suitability of testing methodology and review of issue resolution logs. The auditor may also attend selected IRB and Triage Panel meetings, alongside participating in Test Assurance Board meetings.

The auditor will inform DCC of any observations that are raised during Solution Test within 1 Working Day, such that DCC can initiate corrective action at the earliest possible opportunity. DCC will inform the Panel's Testing

Advisory Group of any such observations and corrective actions, and may request the attendance of the SIT auditor at monthly Testing Advisory Group meetings.

A report on the testing that has been conducted within a Region, including confirmation that the exit criteria have been met, will be provided to DCC no later than 2 Working Days following the completion of SIT for that Region.

DCC and the SIT Auditor will review the report with the Panel's Testing Advisory Group as part of the SIT exit governance process.

DCC shall include the independent auditor’s report as part of the evidence submitted to SEC Parties and the Secretary of State as part of the SIT Completion process.

17.4. Assurance of Testing Tools and Stubs

DCC shall appoint a party or parties to undertake independent assurance assessments of the updates to the following testing tools being updated to support testing for Release 2.0:

(a) ALM

(b) DCC Device Emulator

(c) GIT For Industry tool (GFI)

Where relevant the independent assurance of the readiness of these tools for their use in Release 2.0 will be completed ahead their use in test phases. For example, the assurance of the Device Emulator shall be completed prior to SIT entry, and the report will be required as one of the SIT entry criteria.

17.5. Assurance of 2.4GHz and Sub GHz RF Coverage

DCC shall appoint a suitably competent independent party to review the results of Joint Test Methodology Testing against the acceptance criteria specified in the Joint Test Methodology. The review shall assure that DCC has performed sufficient testing to demonstrate the degree to which Dual Band Communications Hubs meet expectations for RF Coverage.

Version 12.0

APPENDIX AK

SEC Variation Testing Approach Document for SMETS1 Services

Contents

1 Definitions and Interpretations

1.1 In this SEC Variation Testing Approach Document for SMETS1 Services (SMETS1 SVTAD), except where the context otherwise requires, the expressions in the left-hand column within Table 1.1 shall have the meanings given to them in the right-hand column within Table 1.1. Where not defined in this SMETS1 SVTAD, capitalised terms used in this document are set out in Section A of the Amended SMETS1 SEC or in Schedules or Appendices of the Amended SMETS1 SEC.

1.2 Where there are conflicts between this SMETS1 SVTAD and any of the Testing Approach Documents, this SMETS1 SVTAD shall take precedence.

1.3 Where obligations are expressed in respect of DCC Service Providers in this SMETS1 SVTAD, these shall be construed as obligations on the DCC. Where text is included in this SMETS1 SVTAD which does not explicitly place obligations on a Party, the Panel, or Testing Participant, these shall be construed as obligations on the DCC.

Table 1.1 SMETS1 SVTAD Definitions

Term	Meaning
Active Meter Migration Testing (Active MMT)	has the meaning set out in the MTAD.
Additional SR Testing	has the meaning set out in SEC Appendix R the Common Testing Scenarios Document
Amended SMETS1 SEC	means planned changes to the SEC that do not comprise part of a SMETS1 Uplift, and: • in the case of changes to Sections of the Code, those that have most recently been published by the Secretary of State setting out Services in respect of SMETS1 Smart Metering Systems and other provisions relating to SMETS1 Smart Metering Systems that apply in respect of: • the Device Models and/or Device Model Combinations that are being used in testing in respect of IOC, MOC, or FOC, as the case may be and /or • the Device Models and/or Device Model Combinations that are the subject of the DMCT Process; and • in the case of changes to Schedules and Appendices of the Code, the versions that apply in respect of: • the Device Models and/or Device Model Combinations that are being used in testing in respect of IOC, MOC, or FOC, and/or • the Device Models and/or Device Model Combinations that are the subject of the DMCT Process, which are set out in a document published by the Secretary of State entitled “SMETS1 Testing Baseline Requirements Document”.
Capability Release	means each of Initial Operating Capability (IOC), Middle Operating Capability (MOC) and Final Operating Capability (FOC).

Completion Report	means a report that is produced at completion of a Test Phase setting out evidence demonstrating how the criteria for the completion of that Test Phase have been met.
Depth and Breadth of Regression Testing	means the document produced pursuant to Clause 7.7 that sets out the depth and breadth of regression testing planned for a Migration Test Phase and SIT Test Phase relating to the same DMC.
Depth and Breadth of SIT	means the document produced pursuant to Clause 12.7 that sets out the depth and breadth of testing planned to be undertaken for a SIT Test Phase.
Device Model Combination (DMC)	means a combination of SMETS1 Device Models.
Dormant Meter Migration Testing (Dormant MMT)	has the meaning set out in the MTAD.
DMCT EPCL Report	means the report that is prepared pursuant to Clause 20.41.
DMCT Migration Testing (DMCT MT)	means testing undertaken for the purpose of Clause 20.15 (a).
DMCT Non-Standard Test Pack	means a test pack that is not the Standard Dormant DMCT Migration Test Pack or the Standard DMCT Service Reference Variant Test Pack.
DMCT Process	means the process, procedures and testing set out in Clause 20. DMCT stands for Device Model Combination Testing.
DMCT Schedule	means the schedule published pursuant to Clause 20.10.
DMCT Service Reference Variant Testing	means testing undertaken for the purpose of Clause 20.15 (b).
DMCT Status List	means the list produced pursuant to Clause 20.8.
DMCT Testing Report	means the report that is prepared pursuant to Clause 20.34, Clause 20.35 or Clause 20.38 as the case may be.
Energy Supplier	means a holder of an Electricity Supply Licence and / or a Gas Supply Licence.
Entry Criteria	means the criteria that must be met in order for a Test Phase to start.

EPCL means the list of SMETS1 Eligible Product Combinations.

Exit Criteria means the criteria that must be met in order for a Test Phase to complete.

Final Operating Capability (FOC) has the meaning set out in the DCC's delivery plan for SMETS1 services produced pursuant to Condition 13 of the DCC Licence.

In-Scope DMCs means DMCs comprising SMETS1 Smart Metering Systems that are in scope for enrolment which:

a. are not MOC SIT DMCs;
b. are not IOC Migration Testing DMCs; and
c. in the case of FOC, are not DMCs that have been selected for use in a Migration Test Phase and/or a SIT Test Phase, except where the DCC has issued a notification, pursuant to Clause 20.2A, that such a DMC should be included in the DMCT Process.

For this purpose the SMETS1 Smart Metering Systems that are in scope for enrolment are those which, once enrolled, would comprise SMETS1 Meters for which the Secretary of State has concluded that the DCC is required to provide SMETS1 Services (or, if such conclusions have not yet been reached, those for which the Secretary of State is consulting on as being minded to require the DCC to provide SMETS1 Services), and have not subsequently been determined to be out of scope pursuant to Clause 1.9 (b) of Appendix AL.

Initial Operating Capability (IOC) has the meaning set out in the DCC's delivery plan for SMETS1 services produced pursuant to Condition 13 of the DCC Licence.

IOC Migration Testing DMCs means for DMCs that would utilise the operating capability that is delivered at IOC:

a. any DMC against which Migration Testing in respect of a planned entry on the EPCL comprising that DMC has completed; or
b. where Migration Testing has not completed, any DMCs that have been selected for Migration Testing in respect of a planned entry on the EPCL comprising that DMC and have not been de-selected.

Middle Operating Capability (MOC) has the meaning set out in the DCC's delivery plan for SMETS1 services produced pursuant to Condition 13 of the DCC Licence.

Migration Completion Report has the meaning set out in the MTAD.

Migration Dormant Meter Readiness Testing has the meaning set out in the MTAD.

Migration Testing (MT) means:

a. Active Meter Migration Testing;
b. Dormant Meter Migration Testing; and/or;
c. Mixed Meter Migration Testing.

Migration Test Phase has the meaning set out in the MTAD.

Migration Testing Approach means a document that sets out supplementary rights and obligations in relation to Migration

Document (MTAD)	Testing and Migration DUST.
Migration DUST	means a Testing Service provided by the DCC within Device and User System Testing to enable testing of the interactions with the systems and processes used by the DCC to Migrate SMETS1 Installations.
Migration Solution Testing	has the meaning set out in the MTAD.
Mixed Meter Migration Testing (Mixed MMT)	has the meaning set out in the MTAD.
MOC SIT DMCs	means: a. any DMC against which SIT for MOC has concluded and demonstrated that the DCC can successfully process SMETS1 Service Requests and relevant SMETS1 Alerts in respect of that particular DMC in accordance with the Amended SMETS1 SEC; or b. where SIT has not concluded, any DMCs that have been selected for SIT for MOC and have not been de-selected.
Modified DCC Total System	means the DCC Total System as will be modified to enable the delivery of Services as set out in the Amended SMETS1 SEC.
Pre-Integration Testing (PIT)	means a set of tests undertaken by a DCC Service Provider to verify that the part of the Modified DCC Total System being provided by that DCC Service Provider meets the SMETS1 Testing Objective.
Secure Meters Device Models	means SMETS1 ESME Device Models, SMETS1 GSME Device Models, and SMETS1 CH Device Models manufactured by Secure Meters (UK) Ltd (company number 02199653).
SIT Audit	means a review, conducted by the SIT Auditor, of the testing and assurance undertaken by the DCC during a SIT Test Phase.
SIT Auditor	means the independent person appointed pursuant to Clause19.1.
SIT Auditor Report	has the meaning set out in Table 10.1.
SIT Planned Tests	means the tests that result from the Depth and Breadth of SIT document established pursuant to Clause 12.7.
SMETS1 Interface Testing	means the testing activity that further assures, through the involvement of Users, that the part of the Modified DCC Total System that comprises the DCC User Interface operates in accordance with the Amended SMETS1 SEC.
SMETS1 Interface Test Completion Report	has the meaning set out in Table 10.1.

SMETS1 Services	means Services in relation to SMETS1 Smart Metering Systems.
SMETS1 Testing Objective	means the objective set out in Clause 5.
SMETS1 Uplift	means amendment(s) to the Code that are not planned to be delivered as part of a Capability Release or under the DMCT Process and, in the case of more than one amendment, that are planned to be delivered at the same time.
SMETS1 Uplift DCC Testing	means testing by the DCC of any changes to the DCC Total System that would arise as a result of a SMETS1 Uplift.
SMETS1 Uplift DCC Testing Approach Document	means any document produced pursuant to Clause 21 that sets out the approach to SMETS1 Uplift DCC Testing.
SMETS1 Uplift DCC Testing Completion Report	means the report prepared pursuant to Clause 21.11.
SMETS1 Uplift Mandated User Testing	means mandatory testing by one or more Users of all or part of any changes to the DCC Total System that would arise as a result of a SMETS1 Uplift.
SMETS1 Uplift Mandated User Testing Document	means any document prepared pursuant to Clause 21 that sets out the approach to SMETS1 Uplift Mandated User Testing.
SMETS1 Uplift Testing	means SMETS1 Uplift DCC Testing and/or SMETS1 Uplift Mandated User Testing as the case may be.
Standard Dormant DMCT Migration Test Pack	means a set of tests undertaken for the purposes of Clause 20.15 (a) in respect of SMETS1 Installations comprising only Dormant Meters.
Standard DMCT Service Reference Variant Test Pack	means a set of tests undertaken for the purposes of Clause 20.15 (b).
Solution Test	means a test stage within the System Integration Test Phase that will include testing to ensure that changes to existing interfaces, and new interfaces within the solution, as a result of the Amended SMETS1 SEC, work as intended and to confirm that integration of those parts of the Modified DCC Total System that have changed as a result of the Amended SMETS1 SEC has not caused any regression to existing functionality.
System Capacity Testing (SCT)	means additional non-functional tests that assure that the DCC is capable of meeting the SMETS1 Testing Objective.

System Capacity Testing Approach Document (SCTAD) means a document that sets out the supplementary rights and obligations in relation to System Capacity Testing.

Systems Integration Testing (SIT) means a set of tests undertaken by the DCC and the DCC Service Providers collectively to verify that the parts of the Modified DCC Total System being provided by those DCC Service Providers and the DCC operate together in a way that meets the SMETS1 Testing Objective (excluding those parts that are subject to Migration Testing).

TAG has the meaning given in Clause 3.1.

Testing Approach Document(s) means one or more of the Migration Testing Approach Document, and the System Capacity Testing Approach Document.

Test Assurance Board (TAB) means the DCC body established to approve or reject DCC assurance reports relating to code promotion between environments; consider Test Phase Completion Reports; and approve or revoke the issuance of Test Completion Certificates.

Test Completion Certificate has the meaning of a certificate issued by the DCC to a DCC Service Provider when the DCC considers that the DCC Service Provider has met the relevant Exit Criteria for a Test Phase.

Testing Issue Thresholds means the maximum number of extant Testing Issues that may be permitted:

a. at Test Phase exit;
b. in the case of testing undertaken as part of the DMCT Process, at successful test completion; or
c. in the case of testing undertaken as part of SMETS1 Uplift DCC Testing, at successful test completion.

Test Phase means one of the following:

- Pre-Integration Testing (PIT);
- in the case of IOC, System Integration Testing (SIT) in respect of the DMCs that have been selected pursuant to Clause 13 for the Capability Release, excluding any DMC that has subsequently been de-selected from SIT;
- in the case of MOC and/or FOC, System Integration Testing (SIT) in respect of each planned entry on the EPCL for each DMC that has been selected pursuant to Clause 13 for the Capability Release, excluding any DMC that has subsequently been de-selected from SIT;
- In the case of IOC, SMETS1 Interface Testing;
- Active Meter Migration Testing (Active MMT) in respect of a specified planned entry on the list of SMETS1 Eligible Product Combinations;
- Dormant Meter Migration Testing (Dormant MMT) in respect of a specified planned entry on the list of SMET1 Eligible Product Combinations;
- Mixed Meter Migration Testing (Mixed MMT) in respect of a specified planned entry on the list of SMETS1 Eligible Product Combinations; or
- System Capacity Testing (SCT).

Test Stage means a sub-component part of a Test Phase that may be executed sequentially or in parallel with other sub-components within that Test Phase.

Test Traceability Matrix (TTM) means a document employed to map requirements to test cases that is used to demonstrate how the requirements are covered by the test cases.

Work Off Plan	Means a plan produced on completion of a Test Phase or at the completion of Interface Testing, that specifies the outstanding Testing Issues, and the dates by which these Testing Issues should be resolved.

2 General

2.1 This document is the SEC Variation Testing Approach Document for SMETS1 Services.

2.2 Section X11.7 of the Code requires that the DCC and each person other than the DCC that participates in (or is required to participate in) testing under a SEC Variation Testing Approach Document shall comply with the SEC Variation Testing Approach Document.

2.3 Section X11.8 of the Code specifies that Section H14 of the Code (Testing Services) and the Enduring Testing Approach Document shall apply in respect of testing under a SEC Variation Testing Approach Document as if such testing was a Testing Service under Section H14.34 (Modification Implementation Testing); and each participant in such testing shall be deemed to be a Testing Participant for such purposes.

2.4 This SMETS1 SVTAD sets out:

(a) the testing that is required to be undertaken prior to each of IOC, MOC and FOC of the SMETS1 Services and obligations to undertake such testing;

(b) the requirement for the DCC to undertake the DMCT Process; and

(c) the rules to apply to the development of any SMETS1 Uplift DCC Testing and SMETS1 Uplift Mandated User Testing.

3 Testing Approach Documents

3.1 The Testing Approach Documents shall be developed by the DCC. In developing a Testing Approach Document, the DCC shall consult with the Testing Advisory Group of the Panel (**"TAG"**), Parties and other relevant stakeholders prior to the submission of the document to the Secretary of State.

3.2 The DCC shall submit each draft Testing Approach Document to the Secretary of State, indicating:

(a) why the DCC considers the draft to be fit for purpose;

(b) copies of the consultation responses received; and

(c) any areas of disagreement that arose during the consultation process and that have not been resolved.

3.3 The DCC shall comply with any direction given by the Secretary of State to re-consider, re-consult, and/or re-submit the draft document.

3.4 Once a Testing Approach Document has been approved by the Secretary of State, the DCC and each person other than the DCC that participates in (or is required to participate in) testing in the Test Phase to which that Testing Approach Document relates shall comply with that Testing Approach Document.

3.5 The Testing Approach Document for a Test Phase must describe the Parties or other persons who are entitled or required to participate in that Test Phase.

4 Modification of the SMETS1 SEC Variation Testing Approach Document and Testing Approach Documents

4.1 This SMETS1 SVTAD and the Testing Approach Documents shall be modified by the DCC in accordance with any direction to do so made by the Secretary of State. The DCC shall consult with Parties concerning any proposed modification to those documents in accordance with any direction to do so made by the Secretary of State.

4.2 This SMETS1 SVTAD and the Testing Approach Documents may be modified by the DCC following consultation with Parties and other relevant persons, the TAG, the Authority, and the Secretary of State, provided that:

(a) prior to making any such modification, the DCC must present to the Secretary of State a summary of the consultation responses received and an explanation of how the DCC has taken them into account; and

(b) it may not be modified to the extent that the Secretary of State directs otherwise.

4.3 This SMETS1 SVTAD and the Testing Approach Documents may be modified by the DCC without consultation where the modification is of a minor typographical nature or where the modification has no material effect on the rights or obligations of Parties or any other person who is entitled to undertake testing in accordance with this document. Prior to making such changes, the DCC shall provide notice of its intention to do so, together with the intended changes, to relevant stakeholders and the Code Administrator and shall publish such notice on the DCC Website. Additionally, the DCC shall notify relevant stakeholders and the Code Administrator and shall publish the revised document(s) on the DCC Website once the changes have taken effect.

5 SMETS1 Testing Objective

5.1 With the exception of testing undertaken pursuant to Clause 21, the objective of testing undertaken pursuant to this SMETS1 SVTAD (the "**SMETS1 Testing Objective**") is to:

(a) demonstrate that the DCC, the component parts of the Modified DCC Total System and SMETS1 SMSO Systems where used by a SMETS1 SMSO acting in the capacity of DCC Service Provider:

(i) operate; and

(ii) interoperate with User Systems, Active Meters, Dormant Meters and Smart Metering Systems comprising SMETS1 and SMETS2+ Devices,

to the extent necessary for the DCC to comply with the relevant requirements in Sections F, G, H, L, N and P of the Amended SMETS1 SEC;

(b) demonstrate the capability of a User to interoperate with the DCC User Interface that forms part of the Modified DCC Total System before becoming eligible to send Service Requests in respect of SMETS1 Devices; and

(c) provide a service to enable testing of the interactions with the DCC systems and processes used to Migrate SMETS1 Installations.

5.2 The Testing Objective is demonstrated in the following ways:

(a) SIT demonstrates that the individual systems and processes of the Modified DCC Total System can operate together and interoperate with Smart Metering Systems comprising SMETS1 and SMETS2+ Devices to meet the Testing Objective, except where the systems are those referred to in Clause 5.2 (c);

(b) SMETS1 Interface Testing demonstrates that the Modified DCC Total System can interoperate with User Systems;

(c) Migration Testing demonstrates that:

(i) the individual systems of the Modified DCC Total System and SMETS1 SMSO Systems where used by a SMETS1 SMSO acting in the capacity of DCC Service Provider used to Migrate SMETS1 Installations can operate together and interoperate with Active Meters, Dormant Meters, User Systems, and Smart Metering Systems comprising SMETS1 Devices and SMETS2+ Devices to meet the Testing Objective; and

(ii) the systems used by a SMETS1 SMSO that apply a configuration to Dormant Meters and any associated Devices, and/or instruct the upgrade of the firmware on Dormant Meters and any associated Devices, (in each case pursuant to the requirements in clause 4.27 of the Transition and Migration Approach Document) operate and interoperate with Dormant Meters to meet the Testing Objective;

(d) System Capacity Testing demonstrates that the operational performance of the Modified DCC Total System is not adversely affected by the introduction of SMETS1 Services and that the SMETS1 Services will operate at the requisite performance levels;

(e) through the provision of Migration DUST; and

(f) the DMCT Process demonstrates that the DCC's processes and the component parts of the Modified DCC Total System interoperate with SMETS1 Smart Metering Systems and SMETS1 SMSO Systems such that the DCC is able to successfully Migrate SMETS1 Installations and process SMETS1 Service Requests and relevant SMETS1 Alerts in respect of Smart Metering Systems that comprise a particular Device Model Combination in accordance with the Amended SMETS1 SEC.

5.3 Testing shall be performed by the DCC in accordance with Good Industry Practice.

5.4 In order to achieve the SMETS1 Testing Objective the DCC shall undertake testing activities which include the following:

(a) communication tests from Users to SMETS1 Devices and from SMETS1 Devices to Users;

(b) verifying that all other functional changes, in accordance with the relevant requirements in Sections F, G, H, L, N and P of the Amended SMETS1 SEC, operate as intended;

(c) wherever practicable, the use of automated testing;

(d) monitoring and evaluation of all impacts on the Services, including regression testing of the Service, as defined in this SMETS1 SVTAD and the relevant Testing Approach Documents;

(e) monitoring and evaluation of test data used for testing under this SMETS1 SVTAD and the relevant Testing Approach Documents; and

(f) resolution of Testing Issues via the Testing Issue resolution process as set out in Clause 14.

5.5 PIT, SIT, System Capacity Testing and Migration Testing shall be performed in respect of each of IOC, MOC, and FOC. The SMETS1 Testing Objective applies in respect of each of IOC, MOC, and FOC. The DMCT Process shall apply in respect of any In-Scope DMCs and the SMETS1 Testing Objective shall apply in respect of the DMCT Process.

Overlapping of SMETS1 Testing

5.6 The DCC shall not overlap any SIT and SMETS1 Interface Testing without the prior review of the TAG and agreement of the Panel. For MOC and FOC, the DCC may overlap any Migration Test Phase and any SIT Test Phase in respect of the same, or different, planned entries on the EPCL, however when running an end of cycle for a SIT Test Phase the DCC shall use device sets that have exited end of cycle testing for a Migration Test Phase for the same DMC.

6 SMETS1 Security Testing

6.1 Security testing is integral to all Test Phases and shall be undertaken to demonstrate that the Modified DCC Total System remains Secure.

6.2 Security testing shall be managed by the DCC and undertaken in conjunction with the DCC Service Providers in accordance with Good Industry Practice.

6.3 In order to demonstrate the security of the Modified DCC Total System, during testing the DCC shall undertake activities which shall include the following:

(a) ensuring that all security-enforcing functionality has been adequately tested, including user account provisioning and resets, protective monitoring, SMKI/key management, gateway interfaces, and network infrastructure; and

(b) confirming that security needs have been taken into account in the development of test use cases and the subsequent development of test scripts, including testing of all security-relevant 'misuse' cases, i.e. error conditions that would cause a potential security alert to be raised.

6.4 The DCC shall ensure that appropriate security testing in respect of the Modified DCC Total System is performed across all Test Phases, and that it covers both applications and infrastructure. This will be achieved by:

(a) reviewing and approving IT security vulnerability/penetration test approaches and scope;

(b) reviewing testing reports, identifying outstanding Testing Issues, and ensuring that their security impacts are properly considered at TAB approval points;

(c) ensuring that all security functional and non-functional requirements are appropriately tested (or otherwise assured) and evidenced through the use of a traceability matrix for each Test Phase; and

(d) reviewing all identified Testing Issues that impact security to ensure that they are satisfactorily resolved, or where such issues remain outstanding notify the relevant persons before progression to the next Test Phase and/or before live operation.

7 <u>Approach to Testing</u>

7.1 This SMETS1 SVTAD sets out the generic testing requirements for all Test Phases for each of IOC, MOC, and FOC. Where there are specific testing requirements for a Test Phase these shall be set out in this SMETS1 SVTAD or in the Testing Approach Document for that phase.

7.2 The PIT, SIT, SCT, and MT Test Phases shall be conducted for each of IOC, MOC, and FOC.

7.3 SMETS1 Interface Testing shall be conducted for IOC only. Should a material change to the DCC User Interface be proposed as part of MOC and/or FOC, then SMETS1 Interface Testing shall be repeated for that operating capability. Where any change to the DCC User Interface is proposed as part of MOC and/or FOC, the DCC shall consult with the TAG on whether such change is considered to be material. The DCC shall subsequently notify the Secretary of State of the DCC's views and that of TAG as to whether the change is considered to be material. Where directed to do so by the Secretary of State, the DCC shall propose and consult upon the necessary changes to this SMETS1 SVTAD and any relevant Testing Approach Documents to support repeated SMETS1 Interface Testing in respect of MOC and/or FOC, in accordance with Clause 4. Where the Secretary of State has not issued a direction under this Clause 7.3, then Clause 5.2 (b) shall be deemed to have been met by virtue of SMETS1 Interface Testing having been successfully completed for IOC.

7.4 In undertaking testing for a Capability Release, the DCC shall:

(a) include the testing in each SIT Test Phase of the new functionality that is introduced;

(b) for IOC, include regression testing in SIT of the functionality employed in the DCC Live Systems at the point at which regression testing begins;

(c) for MOC and FOC, prior to exiting any SIT Test Phase undertake two functional end of cycle test runs; and

(d) for MOC and FOC, undertake regression testing in accordance with the Depth and Breadth of Regression Testing document for the relevant Test Phase(s) covering both SIT and MT.

7.5 In undertaking regression testing, the DCC shall ensure that the regression testing undertaken is adequate and that it is undertaken in a suitable manner which may include a combination of automated and targeted testing. For IOC, DCC shall consult with the TAG on the scope of regression testing undertaken during each Test Phase. Where the TAG proposes a change to the regression testing undertaken by the DCC, the DCC shall assess the impact of this and where practical shall accommodate the change and inform TAG of its decision. For IOC, should TAG disagree with the DCC's decision, it may refer the matter to the Secretary of State, whose decision shall be final and binding.

7.6 In the case of MOC and FOC, for each Migration Test Phase and SIT Test Phase relating to the same DMC, the DCC shall set out its proposals to the TAG for regression testing in a draft Depth and Breadth of Regression Testing document applicable to that Migration Test Phase(s) and SIT Test Phase. Each Depth and Breadth of Regression Testing document shall include details on planned regression tests, the environment within which they shall be performed, and the codebase on which they shall be run. Any disagreements between the DCC and the TAG regarding the content of the draft Depth and Breadth of Regression Testing document shall be referred to the Secretary of State for decision whose decision shall be final and binding. Such discussion may take place prior to this Clause 7.6 coming into effect.

7.7 In the case of MOC and FOC, for each Migration Test Phase and SIT Test Phase relating to the same DMC, the DCC shall publish on the DCC Website the final version of the Depth and Breadth of Regression Testing document. The published version shall either be the version that TAG did not disagree with or, where TAG did disagree, the version that reflects any decision by the Secretary of State pursuant to Clause 7.6. Where the DCC considers it necessary, the DCC shall prepare an updated version of the Depth and Breadth of Regression Testing document and the procedures set out in Clause 7.6 and this Clause 7.7 shall apply. The DCC may combine the activities described in Clause 7.6 and this Clause 7.7 so that a single Depth and Breadth of Regression Testing document relates to more than one DMC.

8 Generic Testing Activities

8.1 For each of the Test Phases, the DCC shall perform the following activities in accordance with Good Industry Practice:

(a) implement testing infrastructure;

(b) undertake Test Phase planning;

(c) identify test scenarios;

(d) design test scripts;

(e) produce a test specification document;

(f) produce a relevant traceability matrix;

(g) design and prepare test data, and load the test data into the test environment;

(h) prepare a test execution schedule;

(i) execute testing;

(j) perform quality gate reviews;

(k) Testing Issue management;

(l) Testing Issue resolution;

(m) release and configuration management;

(n) test progress reporting;

(o) test assurance;

(p) test completion reporting; and

(q) in addition, for the DCC shall provide support for Users undertaking testing using the Testing Services made available to User, in accordance with Good Industry Practice.

Test principles

8.2 The DCC shall develop its testing methodologies, test scenarios, and regression testing in accordance with Good Industry Practice.

Test Environment

8.3 Testing of SMETS1 Services shall make use of the DCC test environments and shall permit the use of additional cloud-based environments for DCC Service Provider development and integration activities.

8.4 Each DCC Service Provider shall:

(a) establish, maintain, and control their own secure test environments;

(b) design, develop, and support test stubs, test data and test labs that are required for execution of the respective Test Phases; and

(c) ensure the firmware and software versions required for each Test Phase are installed on the SMETS1 Devices that are used for testing.

Environment Management

8.5 The DCC shall manage and communicate to persons participating in a Test Phase any changes and/or fixes arising from production that are to be deployed into the SIT and UIT environments. Such deployments shall be undertaken in accordance with Good Industry Practice.

Timetable for Testing

8.6 Test Phases shall be commenced in the timescales that are necessary to facilitate testing in accordance with the DCC's delivery plan for SMETS1 Services produced pursuant to Condition 13 of the DCC licence.

9 <u>General Requirements for SMETS1 Testing</u>

9.1 The DCC Service Providers shall produce a test plan & test schedule for each Test Phase for the DCC which shall detail:

(a) the extent of testing to be carried out; and

(b) the responsibilities of the DCC Service Providers including the provision of test data.

9.2 Testing Issues logs shall be produced and retained by the DCC detailing all Testing Issues found during test execution.

9.3 An adequate level of regression testing shall be used to test the Modified DCC Total System to ensure defects are not introduced or uncovered as a result of changes made when the software or its environment is changed.

9.4 Where the DCC considers that a Test Phase should complete, or where the DCC considers that code should be promoted from one DCC test environment to another, the DCC shall have its DCC Service Provider produce a report that shall include:

(a) an overview of the testing that was planned, that details the breadth and depth of the planned tests;

(b) information on the actual number of tests run, passed, failed, and not run, mapped to the overview of testing referred to in Clause 9.4 (a);

(c) an explanation of why any tests were not run;

(d) the details of any failed tests, including impact, severity, and quantity;

(e) details on the number and severity of any Testing Issues that were raised;

(f) information on any outstanding Testing Issues and their severity;

(g) specification of the test environment used;

(h) recommendations for any additional tests to be included in subsequent testing; and

(i) lessons learnt during the testing.

9.5 Following receipt of a report as referred to in Clause 9.4, the DCC shall produce a DCC assurance report that shall include:

(a) details of the test assurance activities undertaken by DCC in the Test Phase;

(b) data on tests executed and assured as passed;

(c) an evaluation of whether the governing exit criteria have been met; and

(d) a view on the acceptability of any open Testing Issues and the associated Work Off Plans.

9.6 The DCC assurance report and supporting documentation will be presented to the TAB for their approval or rejection. Where approved, the DCC assurance report shall be provided to the TAG for information. Where requested by a TAG member, the DCC shall also make available supporting documentation including the report referred to in Clause 9.4 and shall include the appropriate confidentiality markings when doing so.

9.7 For SIT, following approval of the report referred to in Clause 9.6 and where the DCC considers that the SIT Test Phase is completed, the DCC shall produce a Completion Report for that Test Phase (as specified in Table 10.1 which shall include the reports produced pursuant to Clause 9.4 and Clause 9.5) and shall provide the Completion Report for the SIT Test Phase to the TAG for recommendation to the Panel. The DCC may combine the activities described in this Clause 9.7 so that a single Completion Report covers the completion of more than one SIT Test Phase. For MOC or FOC, a Completion Report for a SIT Test Phase may also be combined with a Completion Report for a Migration Test Phase where they are in respect of the same planned entry on the EPCL. Furthermore, for MOC or FOC, a Completion Report for a SIT Test Phase and a Completion Report for a Migration Test Phase in respect of the same planned entry on the EPCL may be combined with other Completion Reports in respect of other planned entries on the EPCL. Each Completion Report for a SIT Test Phase shall be accompanied by the SIT Auditor Report (as an Annex) where the report is required to be prepared pursuant to Clause 19, which shall also be provided to the TAG for information.

9.8 Where the DCC considers that code should be promoted from a DCC test environment into production, the DCC shall produce a report setting out the testing that has been undertaken, which shall be provided to such persons or bodies as directed by the Secretary of State.

9.9 The DCC shall discuss with TAG the format and content (including the level of granularity) of any reports that are to be produced pursuant to this Clause 9 in advance of them being produced and sufficiently early such that any information that needs to be reported is captured as part of the DCC’s test activities.

9.10 Prior to promoting code into an environment in which a Testing Participant(s) is undertaking testing, the DCC shall provide to the Testing Participant(s) a release note. The DCC shall provide such release note in advance of promoting such code to enable the Testing Participant(s) to consider any possible impacts.

10 Specific Deliverables

10.1 The DCC shall publish or update published versions of the documents detailed in Table 10.1.

10.2 The structure of the Completion Reports specified in Table 10.1 shall be discussed with the TAG prior to production.

Table 10.1 Specific Deliverables

Deliverable	Description	Created by	Audience	Timing	Where available
SIT Auditor Reports	Using the SIT Auditor as referenced in Clause 19, a range of independent assurance activities shall be conducted and reports relating to said activity shall be produced in accordance with Clause 19 DCC	DCC	Panel / TAG	As determined by the timing for the reports in Clause 19	Provided to Parties in accordance with Clause 13.20
Completion Report for a SIT Test Phase	Evidence of success against the SMETS1 SIT Exit Criteria. For IOC this is a single SIT Test Phase and for MOC and FOC there are multiple SIT Test Phases.	DCC	Panel / TAG	Following TAB approval of SIT Exit for IOC, and each SIT Test Phase exit for MOC, and FOC.	Provided to Parties in accordance with Clause 13.20
SMETS1 Interface Test Completion Report	Evidence of success against the SMETS1 Interface Testing Exit Criteria	DCC	Panel / TAG	As determined by the timing for the completion of SMETS1 Interface Testing	Publish on DCC Website

11 Traceability

11.1 The overall scope of testing in SIT shall be validated by the DCC to ascertain that it is correct through the use of a TTM, assured by the DCC, which shall set out the requirements in Sections F, G, H, L, N and P of the Amended SMETS1 SEC that are to be tested and the associated test scenarios.

11.2 In respect of IOC, the DCC shall assure the TTM (and any subsequent updates to it) in timescales that do not adversely impact upon the timely undertaking of SIT. In respect of MOC and FOC, the TTM shall be assured by the DCC prior to the commencement of SIT for those operating capabilities. If, during SIT, further changes are made to the Sections F, G, H, L, N and P of the Amended SMETS1 SEC, the TTM will be updated to reflect these changes.

11.3 The TTM shall be used by the DCC to track SIT progress and to demonstrate the completion of SIT and shall form a key element of each and every SIT Audit produced pursuant to Clause 19.4 or each and every Completion Report produced pursuant to Clause 19.6 (as the case may be).

12 Test Procedure

12.1 Progression through the Test Phases for SMETS1 Services shall be gated using Entry Criteria and Exit Criteria.

12.2 The generic Entry Criteria for any Test Phase are set out in Clause 12.5. The generic Exit Criteria for PIT and SIT are set out in Clause 12.9.

12.3 Additional specific Entry Criteria and Exit Criteria shall be established for other Test Phases where required. These shall be set out in the relevant Testing Approach Document (with the exception of SIT where, should such specific Entry Criteria or Exit Criteria be required, they shall be set out in this SMETS1 SVTAD). The DCC shall not commence Migration Testing unless the Test Approach Document for that Test Phase has been approved. The DCC shall produce any other Testing Approach Document in timescales that do not have an adverse impact upon the timely undertaking of the Test Phase to which it relates.

12.4 Test Phases may be subdivided into Test Stages. In these circumstances, Entry and Exit criteria may be established at the Test Stage level to support internal DCC Test Stage gating. Where this occurs, this will be specified in the relevant test plan.

Generic Entry Criteria

12.5 The fulfilment of the following generic Entry Criteria is required to permit entry to all Test Phases:

(a) test plan signed off by the DCC;

(b) Test Completion Certificates for any precursor Test Phase issued, unless in accordance with Clause 5.7 it is determined that the Test Phase may overlap;

(c) test specification prepared, including the production of a TTM, with the exception of SIT for IOC;

(d) confirmation that the required test laboratories, SMETS1 Devices, tools, stubs, environments, and data are in place, secure and are ready for testing;

(e) in the case of each SIT Test Phase for MOC or FOC, the DCC has concluded its discussions with TAG for the depth and breadth of testing to be undertaken in accordance with a draft Depth and Breadth of SIT document applicable to the SIT Test Phase (such discussion may take place prior to this Clause 12.5 (e) coming into effect); and

(f) an approval to proceed certificate for the Test Phase has been issued by the DCC.

12.6 For purposes of Clause 12.5 (b) in respect of MOC and FOC, an MT Test Phase in respect of the same planned entry on the ECPL (or any MT Test Phase) shall not be considered to be a precursor to a SIT Test phase in respect of the same planned entry on the EPCL (or any SIT Test Phase).

12.7 For any SIT Test Phase related to MOC and FOC, any disagreements between the DCC and the TAG regarding the content of the draft Depth and Breadth of SIT document (following discussions concluding as per Clause 12.5 (e)) shall be referred to the Secretary of State for a decision, whose decision shall be final and binding. For each of MOC and FOC, the DCC shall publish on the DCC Website the final version of the Depth and Breadth of SIT document. The published version shall either be the version that TAG did not disagree with or, where TAG did disagree, the version that reflects any decision by the Secretary of State. Where the DCC considers it necessary, the DCC shall prepare an updated version of the Depth and Breadth of SIT document and the procedures set out in Clause 12.5 (e) and this Clause 12.7 shall apply.

12.8 In the case of MOC and FOC, the DCC may combine the activities described in Clause 12.5 (e) and Clause 12.7 so that a single Depth and Breadth of SIT document covers more than one SIT Test Phase. For MOC or FOC, a Depth and Breadth of SIT document may also be combined with a Depth and Breadth of MT document (as described in clause 8 of the MTAD) where they are in respect of the same planned entry on the EPCL. Furthermore, for MOC or FOC, a Depth and Breadth of SIT document and a Depth and Breadth of MT document in respect of the same planned entry on the EPCL may be combined with other Depth and Breadth of SIT documents and Depth and Breadth of MT documents in respect of other planned entries on the EPCL.

Generic Exit Criteria for PIT and SIT

12.9 The following generic Exit Criteria are required to exit and complete any PIT and SIT Test Phase:

(a) all planned tests have been executed. In exceptional circumstances, the DCC may propose to de-scope a planned test. Such de-scoping shall be subject to approval by the TAB. In the case of SIT, the DCC shall refer the TAB's recommendation to the Secretary of State and the test shall only be de-scoped if the Secretary of State approves;

(b) the test success rate that is achieved shall be at or above the minimum levels specified in the relevant Testing Approach Document (for the purposes of SIT this is set out in Table 13.1);

(c) the number and severity of any outstanding Testing Issues is at or below the Testing Issue Thresholds specified in Clause 13 for PIT or SIT as appropriate;

(d) test results and other requisite evidence is documented;

(e) test issue logs are produced;

(f) regression testing is successfully completed in accordance with the criteria specified in the relevant Testing Approach Document (for the purposes of SIT this is set out in Table 13.1);

(g) production of Work Off Plans for any outstanding Testing Issues that occurred in the Test Phase;

(h) Work Off Plans from preceding Test Phases have been completed and the associated tests successfully re-run; and

(i) the reports referenced in Clauses 9.4 and 9.5 have been produced and, where specified, the associated Test Completion Certificates have been issued by the DCC.

12.10 Supplementary information on the SIT Exit Criteria (detailed in Clause 12.9) is set out in Table 13.1.

13 <u>SMETS 1 System Integration Testing</u>

Selection of DMCs for use in testing for each of IOC, MOC, and FOC

13.1 Each Supplier Party shall provide the DCC with any information that the DCC reasonably requests relating to the SMETS1 Devices in respect of which it is the current Supplier Party. This information may include:

(a) corresponding SMETS1 Device Models;

(b) configuration settings of the SMETS1 Devices;

(c) DMC quantities;

(d) the number of Smart Metering Systems that the Supplier Party intends to enrol in relation to IOC, MOC, and FOC;

(e) the mapping of numbers of SMETS1 Devices to the associated DMCs; and

(f) notification of any changes or proposed changes to such SMETS1 Devices including to firmware and configuration settings.

13.2 When selecting DMCs for use in testing pursuant to the SMETS1 SVTAD for a Capability Release, the DCC shall do so with the objective of facilitating the enrolment of all SMETS1 Smart Metering Systems that are in scope for enrolment as soon as reasonably practicable. For the purposes of this Clause 13, the SMETS1 Smart Metering Systems that are in scope for enrolment are those which, once enrolled, would comprise SMETS1 Meters for which the Secretary of State has concluded that DCC should be required to provide SMETS1 Services (or, if such conclusions have not yet been reached, those for which the Secretary of State is consulting on as being minded to require DCC to provide SMETS1 Services), and have not subsequently been determined to be out of scope pursuant to Clause 1.9 (b) of Appendix AL.

13.3 For IOC, the DCC shall determine the DMCs with which to start testing pursuant to this SMETS1 SVTAD. For MOC and FOC, the DCC shall determine the DMCs with which to start testing in respect of a SIT Test Phase or a Migration Test Phase pursuant to this SMETS1 SVTAD. Prior to making such a determination, and with the exception of the SMETS1 ESME Device Model component(s) of the DMC(s) for FOC (as further set out in Clauses 13.10 to 13.12), the DCC shall discuss its proposals with stakeholders and set out the rationale for its selection.

13.4 This Clause 13.4 and Clauses 13.5 to 13.9 do not apply in respect of the SMETS1 ESME Device Model component(s) of the DMC(s) for FOC (as to which see Clauses 13.10 to 13.12). For IOC, the DCC shall notify Supplier Parties of the DMCs with which it has decided to start testing. For MOC and FOC, the DCC shall notify Supplier Parties of the DMCs with which it has decided to start testing for particular Test Phases. Where any Supplier Party disagrees with any DCC decision made pursuant to this Clause 13.4, the matter may be referred to the Secretary of State within 10 Working Days of the DCC's decision, and the decision of the Secretary of State shall be final and binding for the purposes of this Code.

DMC De-selection (excluding SMETS1 ESME for FOC and Secure Meters Device Models for MOC)

13.5 Except for Secure Meters Device Models for MOC (as to which see Clauses 13.10 to 13.12), where, having regard to the objective of facilitating the enrolment of all SMETS1 Smart Metering Systems that are in scope for enrolment as soon as reasonably practicable, the DCC considers that a DMC previously selected for use in a Migration Test Phase and/or a SIT Test Phase should be de-selected for such use, then the DCC shall consult with TAG on the de-selection of the DMC from testing, and in so doing shall anonymise and redact information where appropriate.

13.6 Following the TAG consultation, the DCC shall decide whether to de-select the DMC from testing pursuant to this SMETS1 SVTAD and notify the TAG and Supplier Parties accordingly.

13.7 Where a Supplier Party disagrees with the DCC de-selection decision, the Party may refer the issue to the Secretary of State within 10 Working Days of the DCC's decision. Pending the determination by the Secretary of State, the Secretary of State shall inform the DCC as to whether it should continue testing with the DMC in SIT for IOC or in the Migration Test Phase and/or SIT Test Phase for MOC or FOC.

13.8 Where the Secretary of State determines that the DMC should not be omitted from SMETS1 testing, the DCC shall not de-select it from either:

(a) SIT for IOC; or

(b) the SIT Test Phase and/or Migration Test Phase for either MOC or FOC (as the case may be).

13.9 Where the DCC, having taken all reasonable steps to do so, is unable to obtain a selected DMC for use in testing and thus the DCC has proposed de-selection pursuant to Clause 13.5, the DCC shall recommend to the Secretary of State any alternative course of action, having regard to the objective of facilitating the enrolment of all SMETS1 Smart Metering Systems that are in scope for enrolment as soon as reasonably practicable.

Varying Device Models for FOC and MOC Secure

13.10 The SMETS1 ESME Device Model(s) used in respect of Migration Test Phases and SIT Test Phases for FOC shall be the Device Model(s) chosen by DCC from time to time. The Secure Meters Device Models used in respect of Migration Test Phases and SIT Test Phases for MOC may be varied by DCC from time to time. It is acknowledged that the following may need to change as testing progresses:

(a) the SMETS1 ESME Device Model(s) used in Migration and/or SIT Test Phases for FOC; and

(b) the Secure Meters Device Models used in Migration and/or SIT Test Phases for MOC.

When initially choosing the ESME Device Model(s) for FOC, and when changing any of the Device Models referred to in Clause 13.10 (a) or Clause 13.10 (b) in respect of FOC or MOC (as applicable), the DCC shall choose the one(s) that it considers will successfully interoperate with the DCC Systems, and shall have regard to the objective set out in Clause 13.2.

13.11 The DCC shall first notify the SMETS1 ESME Device Model(s) chosen to form component(s) of DMC(s) used in FOC Test Phases alongside its notification made pursuant to Clause 13.4. The DCC shall promptly notify any change in Device Model(s) pursuant to Clause 13.10 (a) or Clause 13.10 (b) and the rationale for such change. Such notifications shall be via the reports produced pursuant to Clause 16.1.

13.12 In the case of FOC, with the exception of references in Clauses 13.3 to 13.11 references in the Code to DMCs selected for use in Migration Test Phases or SIT Test Phases shall be deemed to include the SMETS1 ESME Device Model components from time to time chosen by the DCC pursuant to this Clause 13. In the case of MOC, with the exception of Clauses 13.5 to 13.11, references in the Code to DMCs selected for use in Migration Test Phases or SIT Test Phases shall be deemed to include the DMC(s) including Secure Meters Device Models, determined or chosen from time to time pursuant to this Clause 13.

DCC Witnessing of SIT Testing

13.13 For IOC, the DCC shall produce and maintain a document (the "**SMETS1 SIT Approach Release**"). This document shall contain supplementary information setting out the testing to be undertaken in SIT for IOC including a description of the testing to be undertaken, the scope of planned tests, test methods and test procedures. The DCC shall provide this SMETS1 SIT Approach Release to the TAG as part of the ongoing oversight of SIT for IOC.

13.14 The DCC shall observe a subset of the tests carried out in each and every SIT Test Phase. The subset of tests to be observed shall be selected by the DCC having regard to providing assurance that the Testing Objective has been met.

13.15 The DCC shall observe test execution, and record results produced from executed tests. There shall be:

(a) no deviation from test scripts; and

(b) no involvement by observers in the execution.

13.16 The DCC shall in its Completion Report for a SIT Test Phase describe the results of DCC's witnessing including:

(a) the number of successfully completed tests;

(b) the number and reason for tests that have failed; and

(c) the number of successfully completed tests as a ratio or percentage of the total number of tests executed.

SIT Exit Criteria

13.17 The Exit Criteria in Clause 12.9 apply to any SIT Test Phase and are supplemented with the additional details and additional Exit Criteria set out in Table 13.1. SIT testing shall be performed for each of IOC, MOC, and FOC and these additional details and Exit Criteria will apply for each of IOC, MOC, and FOC.

Table 13.1 SIT Exit Criteria

#	Exit Criteria	Success	Evidence

1A	Functional SIT Execution (For IOC)	For IOC, successful completion will be 100% of planned tests (unless as set out in Clause 12.9 tests have been de-scoped and such de-scoping approved by the Secretary of State) for functional testing have been executed, with a 90% pass rate for any planned tests on the same DMC (excluding those tests that have been de-scoped).	Completion Report for the SIT Test Phase and TAB Test Completion Certificate
1B	Functional SIT Execution (For any SIT Test Phase for MOC and FOC)	For MOC and FOC, successful completion will be 100% of SIT Planned Tests (unless as set out in Clause 12.9 tests have been de-scoped and such de-scoping approved by the Secretary of State) for functional testing have been executed, with a 90% pass rate for any planned tests for the SIT Test Phase (excluding those tests that have been de-scoped).	Completion Report for the SIT Test Phase and TAB Test Completion Certificate
2A	SIT End of Cycle Testing	Successful completion will be 100% of SIT Planned Tests for end of cycle testing established pursuant to Clause 12.7 have been executed, with a pass rate of 100% excluding: 1. defects known at the start of end of cycle testing; 2. any new defects arising since the start of end of cycle testing where such exclusion is approved by the TAG. Where the TAG does not approve exclusion of a new defect in (b) above, the DCC may refer the matter to the Secretary of State for determination. The Secretary of State's determination shall be final and binding for the purposes of this Code.	Completion Report for the SIT Test Phase and TAB Test Completion Certificate
2B	SIT Regression Execution	Successful completion will be 100% of planned tests for regression testing (pursuant to Clause 7) have been executed: 1. for IOC, on the stage exit versions of the software; and 2. for MOC and FOC, in accordance with the relevant Depth and Breadth of Regression Testing, with a 100% pass rate excluding known defects.	Completion Report for the SIT Test Phase and TAB Test Completion Certificate
3	Testing Issue Thresholds	Extant Testing Issues are within the relevant Testing Issue Threshold (Clause 13)	Completion Report for the SIT Test Phase and TAB Test Completion Certificate
4	Test results documented and evidence captured	Results of testing documented and evidence stored	Completion Report for the SIT Test Phase
5	Complete set of Testing Issue logs produced	Logs have been produced and stored for all Testing Issues identified in Testing	Referenced in the Completion Report for the SIT Test Phase
6	Full Test traceability to the requirements	Test Traceability (as defined in the TTM) demonstrated and documented as set out in Clause 11	Completion Report for the SIT Test Phase (where Clause 19.6 applies) or the SIT Auditor Report
7	Full Test traceability of	Test heatmap produced that shows coverage and success of	Completion Report for the

	executed tests	testing, and traceability to the TTM as set out in Clause 11	SIT Test Phase (where Clause 19.6 applies) or the SIT Auditor Report

8	DCC assurance report approved	TAB approval of the DCC assurance report referred to in Clause 9.6	Issuing of a Completion Report for the SIT Test Phase by the TAB for consideration by the Panel

Process for agreeing SIT Completion

13.18 SIT for IOC and each SIT Test Phase for MOC and FOC shall only complete when the Panel determines that the SIT Exit Criteria have been met. When the DCC considers that such completion ought to occur, the DCC shall:

(a) notify the Secretary of State, the Authority, the Panel, and the Parties that the DCC considers that SIT has been completed;

(b) provide the Authority, the Panel, and the Secretary of State with copies of the SIT Completion Report (including any corresponding SIT Auditor Report), and a list of the sections of such reports that the DCC considers should be redacted; and

(c) review the supporting documentation and evidence with regards to the relevant entry and exit criteria with the TAG.

13.19 The Panel shall confirm the completion of SIT, for the Test Phase or shall highlight where it believes the Exit Criteria have not been met. Where the Panel believes the Exit Criteria have not been met, it shall direct the DCC to continue SIT for the Test Phase and to address outstanding matters and submit further documentation and evidence to support the completion of SIT for the Test Phase, following receipt of additional materials the Panel shall determine whether or not SIT for the Test Phase has completed (and this Clause 13.19 shall apply again).

13.20 On direction from the Panel, the DCC shall provide the Parties with copies of the Completion Report (including any corresponding SIT Auditor Report), having first redacted any sections specified by the Panel.

Testing Issue Thresholds

13.21 Testing Issue Thresholds shall be applied as a component of the Exit Criteria for a Test Phase in each of IOC, SMETS1 Interface Testing, MOC, and FOC. Within a Test Phase, all Testing Issues that are raised during that Test Phase or that were raised in any equivalent Test Phase for IOC or MOC, and which remain open shall be counted as extant Testing Issues within that Test Phase for that Test Phase exit or for SMETS1 Interface Testing exit. In addition, in the case of SMETS1 Interface Testing, any extant Testing Issues identified elsewhere across the DCC test environments, or production issues identified in the production environment, which could impact the decision to deploy the SMETS1 code into the production environment will also be assessed and where agreed by TAG shall be treated as extant Testing Issues and included in the overall assessment for SMETS1 Interface Testing exit as further set out in Clause 13.27.

13.22 Except in the case of a Test Phase for SIT for MOC or FOC, the Testing Issue Thresholds per DCC Service Provider in each Test Phase for a Capability Release are set out in Table 13.2 below, with the exception of Testing Issue Thresholds for the Migration Test Phase (which shall be detailed in the MTAD). The Testing Issue severity levels shall be applied where the Testing Issue has arisen as a consequence of the DCC or the Modified DCC Total System and shall be defined by reference to the testing issue severity descriptions in clause 12 of the Common Test Scenarios Document.

Table 13.2 Testing Issue Thresholds per DCC Service Provider

Testing Issue Severity	PIT	SIT (IOC only)	SMETS1 Interface	SCT

			Testing (IOC Only)	
1	0	0	0	0
2	0	0	0	0
3	15	15	5	15
4	30	30	10	30
5	60	60	20	60

13.23 In the case of a Test Phase for SIT for MOC or FOC, the Testing Issue Thresholds set out in Table 13.3 apply. The Testing Issue Thresholds are calculated across all DCC Service Providers collectively and comprise both:

(a) a threshold for the individual Test Phase for SIT; and

(b) an aggregate threshold that takes into account any open Testing Issues for MOC or FOC.

Table 13.3 SMETS 1 SVTAD Testing Issue Thresholds for SIT in the Circumstances of MOC or FOC

Testing Issue Severity	For Clause 13.23 (a) SIT Test Phases for MOC or FOC	For Clause 13.23 (b) Aggregate limit across Test Phases for MOC or FOC
1	0	0
2	0	0
3	15	30
4	30	60
5	60	120

13.24 In the case of a SIT Test Phase for MOC, or FOC, on completion of any SIT Test Phase, any Testing Issues that are open that would affect the functioning of the solution for the planned entry on the EPCL shall be counted for the purpose of the SIT Test Phase for that planned entry on the EPCL, irrespective of the Test Phase in which they arose.

13.25 If during the SIT Test Phase or the SMETS1 Interface Testing Phase, a Testing Issue is opened that the DCC believes should not be counted against the Testing Issue Threshold for that Test Phase, the DCC shall inform the TAB, the TAG, and the Panel; and shall state its rationale for proposing the exclusion. The Testing Issue shall be excluded for the purposes of calculating whether the Testing Issue Threshold has been exceeded only if the TAG agrees. Information on all Testing Issues so excluded from the calculation shall be included in the Completion Report produced pursuant to Clause 16.5.

13.26 Where the DCC's initial exclusion proposal is not supported, the Testing Issue shall be counted when calculating whether the Testing Issue Threshold has been exceeded. Should the TAG and the DCC disagree on the exclusion of a Testing Issue and where this decision has a material impact on the ability to:

(a) deliver IOC; or

(b) complete SIT or MT in respect of a planned entry of the EPCL for either, MOC, or FOC,

the DCC (having regard to the objective of facilitating the enrolment of all SMETS1 Smart Metering Systems that are in scope for enrolment as soon as reasonably practicable) may refer the matter to the Secretary of State, within 5 Working Days of the TAG's decision, for determination. The Secretary of State's decision shall be final and binding for the purposes of this Code.

13.27 In reviewing extant Testing Issues for a SIT Test Phase, the DCC shall discuss with TAG whether any Testing Issues that have been raised in the SCT Test Phase to date, should be counted for the purposes of determining whether the SIT Test Phase Testing Issue Threshold has been exceeded and therefore whether the Testing Issue Threshold exit criterion for the SIT Test Phase has been met.

13.28 In reviewing extant Testing Issues for SMETS1 Interface Testing exit, the DCC shall present:

(a) all open severity 1-3 Testing Issues raised by any Testing Participant; and

(b) all open severity 4-5 Testing Issues raised by any Party that has completed Additional SR Testing of SMETS1 Service Requests or Alerts; and

(c) any other open severity 1-3 issues that have arisen in DCC test or production environments that the DCC believes could impact the decision to deploy the SMETS1 code into the production environment,

to the TAG, to:

(d) confirm that the correct severities have been assigned; and

(e) determine which of the issues in (a), (b) and (c) should be counted for the purposes of determining whether the Testing Issue Threshold has been exceeded and therefore whether the Testing Issue Threshold exit criterion for SMETS1 Interface Testing has been met.

13.29 Should the DCC disagree with the TAG on whether a Testing Issue raised in the SCT Test Phase should be counted under Clause 13.27, or on the matters set out in Clause 13.28 (d) or Clause 13.28 (e), the DCC may refer the matter to the Secretary of State for determination, whose decision shall be final and binding for the purposes of this Code.

Variation to Enduring Test Approach Document

13.30 Clause 7.1(b), 8.3 and 8.4(c) of the Enduring Testing Approach Document shall be varied so that:

(a) Prior to a Device Model Combination being added to the list of Eligible Product Combinations, references to a Device Model Combination that is on the list of Eligible Product Combinations shall include:

(i) a Device Model Combination against which SIT has completed or, where SIT has not completed, a Device Model Combination against which all relevant SIT tests in respect of that DMC have been successfully concluded; and

(ii) a Device Model Combination for which a DMCT Report has been published pursuant to Clause 20 whereby the DCC is recommending that an entry is added to the list of SMETS1 Eligible Product Combinations in respect of that DMC; and

(b) the DCC shall only be required to provide DMCs of the type listed in Clause 7.1(b) and 8.3, and a Testing Participant shall only be entitled to supply its own DMCs in a DCC test lab of the type set out in Clauses 8.4(c), where

(i) SIT has completed against such a type of DMC or, where SIT has not completed, all relevant SIT tests in respect of such a type of DMC have been successfully concluded; or

(ii) A DMCT Report whereby the DCC is recommending that an entry is added to the list of SMETS1 Eligible Production Combinations in respect of that DMC has been published pursuant to Clause 20.

14 <u>Testing Issue Resolution</u>

14.1 The process set out in Section H14.37 onwards of the Code shall apply for the purposes of Testing Issue resolution during SIT, SMETS1 Interface Testing, SCT, and MT; subject to Clause 14.2 and Clause 14.3.

14.2 Where a Testing Participant disagrees with a determination by the DCC pursuant to Section H14.39(a) (with regards to the severity level only) then the matter may be referred to the TAG, whose decision will be final and binding for the purposes of this Code.

14.3 Where the Testing Participant disagrees with the DCC's determination pursuant to Section H14.41 of the matters set out at Section H14.39(c) (but not otherwise), then the Testing Participant may request that the DCC refers the matter to the Secretary of State.

14.4 Except in the circumstances set out in Clause 14.5, where a disagreement exists pursuant to Clause 14.2, the determination of the DCC including assigned Testing Issue severity shall remain and be included in any evaluation until the TAG reaches its determination and notifies the DCC and the Testing Participant for the purposes of this Code.

14.5 If the matter being disputed pursuant to Clause 14.2 could affect whether the Exit Criteria for a Test Phase have been met, a decision on whether the Exit Criteria have been met cannot be made until the TAG determination has been made.

15 Work Off Plans

15.1 At the point of Test Phase exit and, in the case of the SMETS1 Interface Testing test completion, all open Testing Issues shall be documented in a Work Off Plan which shall be approved by the TAB. The Work Off Plan will form part of the underlying evidence considered by the DCC which is referenced in the Completion Report presented for agreement to the Panel. Any Work Off Plans shall set out the following timescales within which all open Testing Issues are to be resolved:

(a) for severity 3 Testing Issues, within 20 Working Days from the issuing of a Test Completion Certificate;

(b) for severity 4 Testing Issues, within 40 Working Days from the issuing of a Test Completion Certificate; and

(c) for severity 5 Testing Issues, within 60 Working Days from the issuing of a Test Completion Certificate.

15.2 The DCC shall monitor the discharge of Work Off Plans and report progress to the TAB. If the timescales for resolution of a Work Off Plan are not going to be met, as soon as reasonably practicable after the person responsible for implementing the Work Off plan becomes aware that this is the case, a correction plan shall be produced and presented to the TAB for its approval. The TAB will consider the correction plan and may elect to revoke any Test Completion Certificate that it has issued pending resolution of the open Testing Issues contained in the correction plan. The resolution of Work Off Plans shall be reported to the TAG and the Panel and the resolution of production issues shall be reported to the Panel.

16 Test Reporting

Weekly DCC Test Execution Report

16.1 The DCC shall provide a weekly test execution report to the Panel and the Secretary of State; the content shall be anonymised and redacted where appropriate.

16.2 The test execution report shall detail progress of testing undertaken pursuant to this SMETS1 SVTAD, including relevant test phases, test issue reporting and capacity.

16.3 During SIT, the test execution report shall, in addition to the requirements specified in Clause 16.1 to Clause 16.2, detail progress of testing and testing coverage of functional areas, including functional groups as detailed in the heatmap.

Completion Reports

16.4 With the exception of PIT, the DCC shall produce Completion Reports covering the matters set out in Table 10.1 where it considers the relevant Exit Criteria for the Test Phase or Exit Criteria for SMETS1 Interface Testing, have been met.

17 Test Resources

Test Stubs

17.1 The DCC may during SIT use a service user simulator Testing Stub to simulate a User.

18 Additional Obligations

All Testing Participants and the DCC

18.1 The DCC and all Testing Participants involved in SMETS1 Services testing undertaken pursuant to this SMETS1 SVTAD shall:

(a) undertake testing in accordance with Good Industry Practice; and

(b) take all reasonable steps to facilitate achievement of the SMETS1 Testing Objective.

The DCC

18.2 The DCC shall ensure that:

(a) test activities are conducted in accordance with this SMETS1 SVTAD and the associated Testing Approach Documents;

(b) test plans are produced and employed;

(c) the necessary test scenarios, test scripts, Test Traceability Matrices, test data, and test environments are put in place;

(d) planned tests are executed and evidence captured;

(e) test issues are documented, diagnosed, and where it is within the remit of the DCC they are resolved;

(f) test progress is monitored and progress is reported;

(g) tests are assured, through witnessing and the review of evidence;

(h) Completion Reports are produced and submitted;

(i) the TAB is managed and supported;

(j) the Panel is supported in making their SMETS1 recommendations and decisions; and

(k) the Secretary of State is supported in making his or her SMETS1 decisions.

19 SIT Audit and Independent Assurance

19.1 The DCC shall appoint an independent SIT Auditor through the existing DCC audit and assurance framework agreement available on the DCC website.

19.2 Tender responses shall be assessed against criteria which inter alia shall include:

(a) independence from the DCC and the DCC Service Providers;

(b) proposed audit approach;

(c) relevant experience; and

(d) cost.

19.3 The identity of the SIT Auditor shall be notified to the Authority, the Panel, Parties, and the Secretary of State following contract award.

19.4 For the SIT Test Phase in respect of the first planned entry on the EPCL in respect of a SMETS1 SMSO, the SIT Auditor shall produce a SMETS1 SIT Audit Report (to accompany the Completion Report for the SIT Test Phase) that shall include:

(a) a review of the Test Traceability Matrix documentation produced by the DCC, to confirm that it provides a mapping of test scenarios to the Code requirements (being those requirements that need to have been tested in order to demonstrate the SMETS1 Testing Objective in Clause 5);

(b) a review of the test heatmap produced by the DCC to confirm that the planned tests map to the test scenarios and test them adequately;

(c) confirmation that DCC testing and assurance has been conducted in accordance with this SMETS1 SVTAD (including confirming its coverage and completeness);

(d) confirmation that each of the test Exit Criteria have been met;

(e) confirmation that all open Testing Issues have been captured and either closed or, where still open, Work Off Plans are in place; and

(f) a view on the acceptability of any open Testing Issues and the associated Work Off Plans.

19.5 In the case of SIT for IOC, the DCC shall require the SIT Auditor to, as soon as reasonably practicable after SIT has commenced, provide an interim opinion on the matters set out in Clause 19.4 (a) and Clause 19.4 (b). This opinion shall reflect the Test Traceability Matrix and heat map in use at that point. DCC shall share and discuss the interim opinion with the TAG.

19.6 The obligation in this Clause 19.6 shall apply in respect of SIT Test Phases in relation to any subsequent planned entries on the EPCL in respect of a SMETS1 SMSO. The DCC shall ensure that the matters prescribed in this Clause 19.6 shall be undertaken by DCC personnel that are sufficiently independent from those undertaking the testing activities. Within each Completion Report for the SIT Test Phase, the DCC shall include:

(a) confirmation that the DCC has assured that the Test Traceability Matrix documentation provides a mapping of test scenarios to the Code requirements (being those requirements that need to have been tested in order to demonstrate the SMETS1 Testing Objective in Clause 5);

(b) confirmation that the DCC has reviewed the test heatmap to confirm that the SIT Planned Tests map to the test scenarios and test them adequately;

(c) confirmation that the DCC's testing and assurance has been conducted in accordance with this SMETS1 SVTAD (including confirming its coverage and completeness);

(d) confirmation that each of the test Exit Criteria have been met;

(e) confirmation that all open Testing Issues have been captured and either closed or, where still open, Work Off Plans are in place; and

(f) a view on the acceptability of any open Testing Issues and the associated Work Off Plans.

19.7 The DCC may combine the activities described in this Clause 19 for several SIT Test Phases undertaken pursuant to this SMETS1 SVTAD into a single set of activities and report to align to each Completion Report where a single report is being produced for those SIT Test Phases pursuant to Clause 13.

20 Process for Device Model Combination Testing (DMCT Process)

20.1 The DCC shall undertake the DMCT Process for any In-Scope DMCs and shall do so in timescales and in a manner designed to facilitate the enrolment of all SMETS1 Smart Metering Systems that are in scope for enrolment as soon as is reasonably practicable. For this purpose and for the purpose of Clause 20.2A, the SMEST1 Smart Metering Systems that are in scope for enrolment are those which, once enrolled, would comprise SMETS1 Meters for which the Secretary of State has concluded that the DCC is required to provide SMETS1 Services (or, if such conclusions have not yet been reached, those SMETS1 Smart Metering Systems for which the Secretary of State is consulting on as being minded to require the DCC to provide SMETS1 Services), and have not subsequently been determined to be out of scope pursuant to Clause 1.9 (b) of Appendix AL.

20.1A Clause 20.1 shall not apply in respect of any In-Scope DMCs that comprise (or would comprise) SMETS1 Smart Metering Systems in respect of a SMETS1 SMSO for which the RP Decommissioning Date for the associated Requesting Party has expired. Where the DCC is partway through the DMCT Process in respect of such DMCs at the point at which the RP Decommissioning Date expires, the DCC shall not continue the DMCT Process in respect of those DMCs. Additionally, Clause 20.2 shall not apply in respect of any SMETS1 Smart Metering Systems that comprise (or would comprise) Smart Metering Systems in respect of a SMETS1 SMSO for which the RP Decommissioning Date for the associated Requesting Party has expired.

20.2 A Supplier Party may notify the DCC of any SMETS1 Smart Metering Systems that the Supplier Party is planning to enrol excluding:

(a) Smart Metering Systems that are comprised of an MOC SIT DMC or an IOC Migration Testing DMC; and

(b) in the case of FOC, Smart Metering Systems that comprise a DMC that has been selected for use in a Migration Test Phase and/or a SIT Test Phase pursuant to Clause 13, except where the DCC has notified Supplier Parties pursuant to Clause 20.2A that such a DMC is to be included in the DMCT Process.

Where a Supplier Party wishes to so notify the DCC, the Supplier Party shall contact the DCC via an email to SMETS1DMCT@smartdcc.co.uk to advise of their intent. The DCC shall respond within 10 working days following receipt by the DCC, stating the data reasonably required by the DCC for the purposes of this Clause 20, and a reasonable format for the submission. Each Supplier Party shall ensure that it provides in its submission to the DCC the most accurate and up to date data. The DCC shall be entitled to rely upon the data notified for the purposes of this Clause 20.

20.2A In the case of FOC, the DCC shall include within the DMCT Process any DMC that has been selected for use in a Migration Test Phase and/or a SIT Test Phase where the DCC considers that doing so would facilitate the enrolment of all SMETS1 Smart Metering Systems that are in scope for enrolment as soon as reasonably practicable. Where this is the case, the DCC shall notify each Supplier Party that is an Installing Supplier (as defined in the Transition and Migration Approach Document) of Smart Metering Systems comprising the DMC that such DMC is also to be included in the DMCT Process.

20.3 For any particular submission required to be made pursuant to Clause 20.2, where a Supplier Party confirms in writing to the DCC that the most recently submitted data applies to the current submission, then the Supplier Party shall not be required to resubmit the data that has remained unchanged. For the purposes of this Clause 20.3, a Supplier Party shall be entitled to refer to any data submitted to the DCC prior to this Clause 20 coming into effect.

20.4 Where a Supplier Party has been unable to provide part of the data requested pursuant to Clause 20.2, the DCC shall take all reasonable steps to obtain the data from the relevant Meter Manufacturer and/or SMETS1 SMSO. Additionally, for the purposes of undertaking the DMCT Process, the DCC shall source data relating to SMETS1 Installations comprising all or part Dormant Meters from SMETS1 SMSOs acting in the capacity of DCC Service Provider.

20.5 Subject to clause 20.5 A, where the DCC is unable to source all of the data that it reasonably requires, then the DCC shall be entitled to exclude the impacted DMC from the remainder of the DMCT Process, and the DCC shall notify any Supplier Party that included the DMC in its submission accordingly. The Supplier Party may include

Device Model Combinations for which the DCC has not been able to source all data required in subsequent submissions made pursuant to Clause 20.2.

20.5A Where a Device Model initially included as a SMETS1 PPMID in a Device Model Combination for the purposes of the DMCT Process is determined by the DCC, pursuant to the definition of a SMETS1 PPIMD as varied by Clause 3.1 (g) of Appendix AL, not to be a SMETS1 PPMID then the DCC shall proceed with the DMCT Process on the basis that the Device Model is deemed to have been included in the DMCT Process as a SMETS1 IHD. Where the Device Model was included as a SMETS1 PPMID in a Device Model Combination by a Supplier Party pursuant to Clause 20.2, the DCC shall promptly notify any Supplier Party of the reclassification of the SMETS1 PPMID Device Model as a SMETS1 IHD, together with the associated rationale. Where any Supplier Party disagrees with the reclassification to a SMETS1 IHD, the matter may be referred to the Secretary of State within 10 Working Days of the DCC's notification to that Supplier Party, and the decision of the Secretary of State shall be final and binding for the purposes of this Code.

20.6 Where all of the data required by the DCC has been provided to, or sourced by, the DCC, or following the process set out in Clause 20.5A, the DCC shall then consider:

(a) whether the DMC proposed for testing is already on the list of SMETS1 Eligible Product Combinations or is already proposed for addition onto that list;

(b) whether the DMC is currently:

(i) an MOC SIT DMC;

(ii) a DMC selected for use in a SIT Test Phase and/or a Migration Test Phase for FOC which has not been notified by the DCC as a DMC that should also be included in the DMCT Process pursuant to Clause 20.2A;

(iii) an IOC Migration Testing DMC; or

(iv) being tested in PPCT;

(c) whether Migration Testing and SIT in respect of the Capability Release of which the DMC will form a part are unlikely to be completed in timescales that would allow the testing of the DMC to be scheduled with a reasonable degree of confidence;

(d) whether, in the DCC's opinion, the DMC proposed is substantively equivalent to:

(i) an entry for an existing DMC that is on the list of SMETS1 Eligible Product Combinations;

(ii) an entry for a DMC that is proposed for addition onto the list of SMETS1 Eligible Product Combinations; or

(iii) a DMC that is planned for testing;

(e) whether the DCC has been unable to source suitable devices for testing (which may include sourcing them for Supplier Parties), or does not yet know whether it can source them; and

(f) whether, in the DCC's opinion, it is not economic to test the DMC.

20.7 The DCC may propose to the Secretary of State any DMC which, in the DCC's opinion, should not be tested on the grounds that it is not economic to test. Prior to making such proposals the DCC shall first discuss with stakeholders its views and the associated rationale and invite stakeholder views. As part of the proposals submitted by the DCC to the Secretary of State, the DCC shall include any stakeholder views received. The decision of the Secretary of State as to whether the DCC should test the DMC shall be final and binding for the purposes of this Code. Where the Secretary of State agrees with the DCC's proposal, the DCC shall exclude the DMC from this DMCT Process. Where the Secretary of State disagrees with the DCC's proposal, the DCC shall continue to progress the DMC through the DMCT Process.

20.8 The DCC shall publish and keep up to date a list ('a DMC Status List') that shows the status of the DMCs in the DMCT Process. The DCC shall change the classification of the status of the DMC on the DMCT Status List as it progresses through the DMCT Process.

20.9 The DCC shall include within a schedule ("the DMCT Schedule") those DMCs for which the DCC is reasonably confident of the proposed dates for testing along with:

(a) the planned start and completion dates for testing of any planned entries on the SMETS1 Eligible Production Combinations that are comprised of that DMC (together with details of those entries) and either;

(b) the test pack planned to be used for DMCT Migration Testing and DMCT Service Reference Variant Testing (as further set out in Clauses 20.16 and 20.17); or

(c) where the DCC proposes to use a DMCT Non-Standard Test Pack in respect of a DMC, the rationale for doing so; and

the DCC shall publish any changes from the previously published DMCT Schedule. Where the DCC is planning to test in respect of an EPCL entry for a SMETS1 Installation that comprises only Dormant Meters, the DCC may choose not to additionally test entries for the same DMC in respect of SMETS1 Installations that comprise Active Meters or both Dormant and Active Meters where it considers that the testing in respect of the entry containing only Dormant Meters will suffice.

20.10 The DCC shall publish the DMCT Schedule (and any subsequent updates to it) on the DCC Website and shall notify Supplier Parties, the SEC Panel, the Authority and the Secretary of State of its publication (and of any update to it). The DCC shall also provide the DMCT Schedule (and any updates to it) to SECAS for publication on the SEC Website.

20.11 For those DMCs that are on the DMCT Status List but where the DCC considers that testing is not required and so is not planned, or testing is planned but the DCC is not reasonably confident of the proposed date for testing, or testing is not planned as the DCC cannot source test devices, the DCC shall notify any Supplier Party that included the DMC in its submission that it has been excluded from the DMCT Schedule indicating:

(a) which of the reasons in Clause 20.6 (a) to 20.6 (e) apply; and

(b) in the case of Clause 20.6 (c), 20.6 (d) or 20.6 (e) the associated rationale.

Such notification shall also be published on the DCC Website and provided to Supplier Parties by the DCC prior to the next submission of information to the DCC pursuant to Clause 20.2.

20.12 Within 20 Working Days of the notification by the DCC to the Supplier Party pursuant Clause 20.11, where a Supplier Party that included a DMC in its submission to the DCC pursuant to Clause 20.2 disagrees with the DCC's decision that:

(a) the DMC proposed is substantively equivalent to an entry for an existing DMC that is on the list of SMETS1 Eligible Product Combinations or is already proposed for addition onto that list or is planned for testing, then the Supplier Party shall notify the DCC (including the rationale for their disagreement) and the DCC shall update the DMCT Schedule to include planned testing of that DMC; or

(b) Migration Testing and / or SIT in respect of the Capability Release of which the DMC will form a part are unlikely to be completed in timescales that would allow DCC to schedule the testing of the DMC with a reasonable degree of confidence, then the Supplier Party shall notify the DCC (including the rationale for their disagreement) and the DCC shall refer the matter to the Secretary of State for determination and the DCC shall update the DMCT Schedule to include planned testing of the DMC where directed to do so by the Secretary of State.

20.12A Where planned testing of a DMC is included in the DMCT Schedule pursuant to Clause 20.12 (a) but the DCC disagrees and considers that testing is not required for the reason in Clause 20.6 (d), the DCC may refer the matter to the Secretary of State for determination, in which case the DCC shall provide the associated rationale for its position to the Secretary of State as part of the referral, and the DCC shall update the DMCT Schedule to remove the planned testing of the DMC where directed to do so by the Secretary of State, in which case the DCC may continue to progress the DMC through the DMCT Process on the basis of Clause 20.6 (d). The DCC must notify any Supplier Party that included the DMC in its submission to the DCC pursuant to Clause 20.2 that it has referred the matter to the Secretary of State and provide the associated rationale for its view that testing is not required.

Tests undertaken against a DMC

20.13 When testing in respect of a planned entry on the EPCL in respect of a DMC, the objective of the tests shall be to verify that:

(a) the DCC can successfully Migrate SMETS1 Installations that are comprised of the DMC; and

(b) once Enrolled, the DCC can successfully process SMETS1 Service Requests and relevant SMETS1 Alerts in respect of Smart Metering Systems that are comprised of the DMC (in whole or in part).

20.14 Where the DCC considers that the DCC Systems used to Migrate SMETS1 Installations comprising the DMC should be tested under Migration Testing pursuant to the MTAD, the DCC shall notify the TAG along with the associated rationale. In circumstances where Migration Testing is not going to be undertaken pursuant to the MTAD for the DMC, the DCC shall execute DMCT MT and DMCT SRVT for that DMC. However, in the alternate case, the DCC shall only be required to execute DMCT SRVT and may do so once the TAB has determined that the Migration Test Phase for the DMC under the MTAD has been completed. Notifications for the purposes of this Clause 20.14 may take place prior to this Clause coming into effect.

20.15 Subject to Clause 20.17 when undertaking:

(a) DMCT MT, the DCC shall execute the Standard Dormant DMCT Migration Test Pack for the Capability Release; and

(b) DMCT SRVT, the DCC shall execute the Standard DMCT Service Reference Variant Test Pack for the Capability Release.

20.16 Each standard test pack referred to in Clause 20.15 shall set out the tests which shall be executed as part of that test pack for the relevant Capability Release. The test pack in respect of each Capability Release shall be proposed by the DCC and agreed with the TAG. Where the DCC and the TAG cannot reach agreement, the DCC may refer the matter to the Secretary of State, whose decision shall be final and binding for the purposes of this Code.

20.17 The DCC may propose to execute a different set of tests (a DMCT Non-Standard Test Pack) for DMCT MT and/or DMCT SRVT in respect of a particular DMC. Prior to doing so, the DCC shall discuss the proposed set of tests with the TAG and seek agreement from the TAG. Where the DCC and the TAG cannot reach agreement on the set of tests which shall be executed and contained within the relevant test pack(s), the matter may be referred to the Secretary of State by the DCC, whose decision shall be final and binding for the purposes of this Code.

20.18 Where the versions of the DCC Systems and environments against which DCC is planning to execute tests (pursuant to this Clause 20) are not the ones that most closely match those that are (or will be) in the production environment at the time at which the Smart Metering Systems that are comprised of the DMCs that are being tested will be eligible to be Migrated, then the DCC shall discuss its proposals with the TAG and shall only execute tests against the alternate version of the DCC Systems and environments if the TAG agrees.

20.19 Once testing in respect of a particular DMC has commenced, the DCC shall be relieved of its obligations to complete testing of a DMC pursuant to this Clause 20 should it no longer have sufficient devices available for use in testing. Where this is the case, the DCC shall notify all Supplier Parties, the Panel, the Authority and the Secretary of State. Such DMCs may be included in a subsequent Supplier Party submission pursuant to Clause 20.2.

DMCT Testing Issues

20.20 Where a DMCT Testing Issue arises whilst executing tests under the DMCT Process which could result in one or more of:

(a) a change to the DCC Internal Systems but no change to the Code; or

(b) a change to the DCC Systems and a change to the Code; or

(c) a change to a SMETS1 Device; or

(d) a change to the Code (but no change to the DCC Systems),

the DCC shall discuss the issue with affected stakeholders and recommend which of the above options should be followed, notifying stakeholders, the SEC Panel, the Authority and the Secretary of State of its recommendation.

20.21 When progressing a DMCT Testing Issue pursuant to Clause 20.20, where appropriate the DCC may pause (and recommence) the DMCT Process (including testing) for the impacted DMC(s). Where the DMCT Process is paused (or recommenced), the DCC shall inform the Panel and the Secretary of State via the reports produced pursuant to Clause 16.1.

20.22 Where the DCC recommends that the option in Clause 20.20 (a) is followed, the DCC shall:

(a) where there is no material impact to the timescales for testing the DMC (or other DMCs), progress the change to the DCC Internal Systems in accordance with Section H8.9 to H8.12, re-run the test pack accordingly and update the DMCT Schedule with the revised completion dates in respect of the DMC(s); or

(b) where there is a material impact to the timescales for testing the DMC (or other DMCs), progress the change to the DCC Internal Systems in accordance with Section H8.9 to H8.12, re-run the test pack accordingly and update the DMCT Schedule with the revised completion dates in respect of the DMC(s), unless the Secretary of State directs otherwise. Where the Secretary of State directs otherwise, the DCC shall comply with any alternative course of action set out in such direction.

The DCC shall inform SEC Parties, the Panel, the Authority and the Secretary of State which of (a) or (b) above that the DCC is planning to undertake in advance of doing so.

20.23 Where the DCC's recommendation is that the option in Clause 20.20 (b) is followed, the DCC shall first consult with the Secretary of State as to whether, in his opinion, the Code change should be consulted upon. Where the Secretary of State agrees that the change ought to be consulted upon the DCC shall propose an approach for testing for agreement by the TAG. The proposed approach shall include:

(a) the DCC’s approach to testing the change (including when and where testing should be undertaken, the tests to be undertaken and the approach to regression testing), rules for test completion and the associated governance; and

(b) an indication of whether testing by Users is required.

Where the Secretary of State does not agree that the Code change should be consulted upon, the DCC shall reconsider and recommend an alternative option for resolving the Testing Issue from the options outlined in Clause 20.20.

20.24 Where an approach for testing (pursuant to Clause 20.23) cannot be agreed by the DCC and the TAG, the matter shall be referred to the Secretary of State for determination whose decision will be final and binding for the purpose of this Code. The DCC shall undertake testing in accordance with the approach and governance as agreed with the TAG or determined by the Secretary of State (as the case may be).

20.25 Where the DCC's recommendation is that the option in Clause 20.20 (c) is followed it shall recommend this to the Secretary of State indicating whether it considers a firmware upgrade or a configuration change or both is required. Where the Secretary of State agrees with the DCC's recommendation and the change requires:

(a) a firmware upgrade, the DMCT Process shall no longer be undertaken in respect of that DMC; or

(b) a change to the configuration applied to a Device or Devices that comprise part of the DMC, the DMC shall be excluded from the DMCT Process until such time as evidence can be provided by any Supplier Party proposing its inclusion (through a subsequent request for information pursuant to Clauses 20.2 and/or 20.3) that the change has been applied or will be applied prior to enrolment; or

(c) a firmware upgrade and a change to the configuration applied to a Device or Devices that comprise part of the DMC, the DMC that results from the new firmware version shall be excluded from the DMCT Process until such time as evidence can be provided by any Supplier Party proposing its inclusion (through a subsequent request for information pursuant to Clauses 20.2 and/or 20.3) that the configuration change has been applied or will be applied prior to enrolment.

20.26 Where the Secretary of State disagrees with the recommendation of the DCC that the option in Clause 20.20 (c) should be followed, the DCC shall reconsider and recommend an alternative option for resolving the Testing Issue from the options outlined in Clause 20.20.

20.27 Where the DCC's recommendation is that the option in Clause 20.20 (d) is followed, but the Secretary of State has indicated that such change(s) should not be progressed, then the DCC shall reconsider and recommend an alternative option from the options outlined in Clause 20.20.

DMCT Testing Exit Criteria

20.28 Testing under the DMCT Process in respect of a planned entry on the EPCL cannot successfully complete where the open Testing Issues in respect of that planned entry on the EPCL exceed the thresholds set out in Table 20.1. The Testing Issue Thresholds are calculated across all DCC Service Providers (including the relevant SMETS1 SMSO, acting in the capacity of DCC Service Provider) collectively and comprise both:

(a) a threshold for the individual planned entry on the EPCL that is the subject of testing under the DMCT Process; and

(b) an aggregate threshold that takes into account any open Testing Issues, irrespective of where they arose.

Table 20.1 SMETS 1 SVTAD Testing Issue Thresholds for DMCT

Testing Issue Severity	For Clause 20.28 (a) Planned entry on the EPCL	For Clause 20.28 (b) Aggregate limit across DMCT
1	0	0
2	0	0
3	15	30
4	30	60
5	60	120

20.29 If there are any open Testing Issues that the DCC believes should not be counted against the Testing Issue Thresholds for the purposes of Clause 20.28 in respect of a planned entry on the EPCL, including where the DCC considers that the open Testing Issues would not affect the functioning of the solution for the planned entry on the EPCL, the DCC may propose to exclude such Testing Issue(s) from its count. Where the DCC proposes to exclude such Testing Issue(s) from its count, the DCC shall:

(a) describe the Testing Issue(s) that it proposes to exclude and the DCC's rationale for exclusion in a draft DMCT Testing Report; and

(b) provide the TAG with a description of the Testing Issue(s) excluded and the DCC's rationale for exclusion for the TAG to review pursuant to Clause 20.38.

20.30 The DCC shall provide the TAG with a description of all open Testing Issues in respect of a planned entry on the EPCL and their assigned severity, indicating whether the extant Testing Issues exceed the relevant Testing Issue Thresholds (pursuant to Clause 20.28).

DMCT Testing Completion

20.31 Where testing is required under the DMCT Process for a planned entry on the EPCL, the DCC shall not produce a draft DMCT Testing Report (pursuant to Clause 20.34 or Clause 20.35 as the case may be) until testing has completed (as determined in Clause 20.32 or Clause 20.33 as the case may be).

20.32 Testing for a planned entry on the EPCL shall be considered to have been completed and to be successful when:

(a) all DMCT Process tests related to the planned entry on the EPCL have been executed;

(b) all Testing Issues raised during testing of the planned entry on the EPCL have been through the processes outlined in Clauses 20.20 to 20.27, as applicable;

(c) where, pursuant to Clause 20.14 the DCC has undertaken Migration Testing for the planned entry on the EPCL pursuant to the MTAD, the Panel has determined that the Migration Test Phase for the planned entry on the EPCL has completed; and

(d) subject to Clause 20.28, any extant Testing Issues do not exceed the relevant Testing Issue Threshold.

20.33 Testing for a planned entry on the EPCL shall be considered to have been completed and to be unsuccessful either,

(a) when:

(i) all DMCT Process tests related to the planned entry on the EPCL have been executed;

(ii) all Testing Issues raised during testing of the planned entry on the EPCL have been through the processes outlined in Clauses 20.20 to 20.27, as applicable;

(iii) subject to Clause 20.28, extant Testing Issues exceed the relevant Testing Issue Threshold; and/or

(iv) where, pursuant to Clause 20.14 the DCC has undertaken Migration Testing for the planned entry on the EPCL pursuant to the MTAD, the Panel has determined that the Migration Test Phase for the planned entry on the EPCL has not completed; or

(b) when it was not possible for all DMCT Process tests related to the planned entry on the EPCL to be executed having been through the processes outlined in Clauses 20.20 to 20.27, or where Migration Testing was planned pursuant to Clause 20.14 and it is not possible to complete it, or where a blocking defect has arisen and the Secretary of State agrees that testing should not continue.

DMCT Testing Reports

20.34 Where the DCC has undertaken testing in respect of the proposed entry on the EPCL and testing has completed successfully, prior to producing the associated DMCT EPCL Report for the purposes of Clause 20.41, the DCC shall produce a draft DMCT Testing Report which shall include:

(a) the version of the DCC Systems and environments against which tests were executed, which, subject to Clause 20.18, shall be those versions and environments that most closely match those that are or will be in the production environment at the time at which Smart Metering Systems that are comprised of the DMC are eligible to be Migrated;

(b) the tests run as per the relevant test pack;

(c) the results of the tests run;

(d) confirmation that all open Testing Issues have been captured and either closed, or where still open, Work Off Plans are in place;

(e) the approach to re-running tests following the deployment of any fixes during testing;

(f) details for any Testing Issues that were excluded pursuant to Clause 20.29 including the rationale for exclusion;

(g) supporting detail setting out the rationale for the severity assigned to any open Testing Issues and the associated Work Off Plans (excluding any Testing Issues reported pursuant Clause 20.34 (f));

(h) any other information as prescribed in the relevant test pack; and

(i) a statement of why the planned entry on the EPCL has successfully completed testing (including, where relevant, reference to any Migration Completion Report).

20.35 Where testing under the DMCT Process has completed unsuccessfully pursuant to Clause 20.33 and therefore the DCC is not proposing a corresponding entry on the EPCL, the DCC shall produce a draft DMCT Testing Report which shall include.

(a) the version of the DCC Systems and environments against which tests were executed, which, subject to Clause 20.18, shall be those versions and environments that most closely match those that are (or will be) in the production environment at the time at which the Smart Metering Systems that are comprised of the DMC are eligible to be Migrated;

(b) the tests run as per the relevant test pack;

(c) the results of the tests run;

(d) confirmation that all open Testing Issues have been captured and either closed, or where still open, Work Off Plans are in place;

(e) the approach to re-running tests following the deployment of any fixes during testing;

(f) details for any Testing Issues that were excluded pursuant to Clause 20.29 including the rationale for exclusion;

(g) supporting detail setting out the rationale for the severity assigned to any open Testing Issues and the associated Work Off Plans (excluding any Testing Issues reported pursuant Clause 20.35 (f));

(h) any other information as prescribed in the relevant test pack; and

(i) a statement of why the planned entry on the EPCL has unsuccessfully completed testing (including, where relevant, reference to any Migration Completion Report).

20.36 The DCC shall make available each draft DMCT Testing Report to any Supplier Party that was planning to enrol one or more SMETS1 Installations that are comprised of the planned entry on the EPCL that is the subject of the DMCT Testing Report (based on the information provided pursuant to Clause 20.2). In addition to the notice provisions set out in Section M10 of the Code, the DCC shall also use any additional contact details provided to DCC pursuant to Clause 20.2 when making available the draft DMCT Testing Report. Such notification of additional contact details by the Supplier Party can include notifications made in submissions received pursuant to Clause 20.2 prior to this Clause 20.36 coming into effect.

20.37 Where a draft DMCT Testing Report has been provided to a Supplier Party pursuant to Clause 20.36 and that Supplier Party considers that a different determination on the successful completion or unsuccessful completion should be arrived at, or might be arrived at because:

(a) the approach to re-running tests following the deployment of any fixes during testing is considered inappropriate;

(b) one or more Testing Issues should not have been excluded pursuant to Clause 20.29; and/or

(c) the severity assigned to one or more Testing Issues should be reduced or increased (as the case may be);

that Supplier Party may (within 10 Working Days of the relevant draft DMCT Testing Report being provided) refer the matter to the Secretary of State for a determination (pursuant to Clause 20.40), setting out its supporting arguments.

20.38 Where the TAG considers that a different determination of the number or severity of the extant Testing Issues against the relevant Testing Issue Thresholds should be arrived at, or might be arrived at, because:

(a) the TAG considers that the severity of one of more of the open Testing Issue(s) (provided pursuant to Clause 20.30) should change; and/or

(b) the TAG disagrees with the exclusion of one or more Testing Issues (where the details were provided to the TAG pursuant to Clause 20.29 (b)),

and that different determination would result in the status of testing changing from successful to unsuccessful, then the DCC shall either:

(c) continue testing under the DMCT Process for the relevant planned entry on the EPCL (and Clause 20.13 onwards shall apply again) and notify any Supplier Party that was provided with the draft DMCT Testing Report accordingly; or

(d) refer the matter to the Secretary of State for determination (pursuant to Clause 20.40).

20.39 Where,

(a) each Supplier Party that received a draft DMCT Testing Report (pursuant to Clause 20.36) has confirmed to the DCC that they will not refer the matter to the Secretary of State for a determination (pursuant to Clause 20.37), or no referral has been made within 10 Working Days (pursuant to Clause 20.37);

(b) any TAG disagreement with the DCC's proposed excluded open Testing Issues (pursuant to Clause 20.38) would not result in changing the status of testing from successful to unsuccessful; and

(c) any TAG disagreement with the severity assigned to open Testing Issues (pursuant to Clause 20.38) would not result in changing the status of testing from successful to unsuccessful,

the draft DMCT Testing Report shall be updated as necessary and deemed to be final.

20.40 Where a referral has been made by a Supplier within 10 Working Days (pursuant to Clause 20.37) and/or by the DCC (pursuant to Clause 20.38) the determination of the Secretary of State shall be final and binding for the purposes of this Code as follows:

(a) where the Secretary of State agrees with the DCC's treatment of the matters in the draft DMCT Testing Report that have been referred by the Supplier Party and/or the DCC, the draft DMCT Testing Report shall be deemed to be final;

(b) where the Secretary of State disagrees with the DCC's treatment of any of the matters in the DMCT Testing Report and as a consequence the status of the testing changes to successful (as referred to in Clause 20.32) the DCC shall update the draft DMCT Testing Report and it shall be deemed to be final; and/or

(c) where the Secretary of State disagrees with the DCC's treatment of any of the matters in the DMCT Testing Report and as a consequence, the status of the testing changes to unsuccessful (as referred to in Clause 20.33) or further tests need to be run, as determined by the Secretary of State, either,

(i) the DCC shall update the draft DMCT Testing Report and it shall be deemed to be final; or

(ii) the DCC shall continue testing under the DMCT Process for the relevant planned entry on the EPCL (and Clause 20.13 onwards shall apply again).

DMCT EPCL Reports

20.41 Where the DCC considers that an entry on the EPCL should be made in respect of a particular In-Scope DMC as a result of the DMCT Process, it shall produce a DMCT EPCL Report:

(a) specifying the proposed entry for the EPCL; and

(b) setting out why the DCC considers that the entry should be made including, where applicable:

(i) a final DMCT Testing Report which provides for successful completion for the proposed entry on the EPCL; or

(ii) a reference to a prior final DMCT Testing Report or other Completion Reports that are relevant for the proposed entry on the EPCL.

For the avoidance of doubt, a DMCT EPCL Report is also required where testing of the DMC under the DMCT Process is not required (as the DCC considers that a planned entry on the EPCL is substantially equivalent pursuant to Clause 20.6 (d) and the DCC's view has not been over-ridden pursuant to Clauses 20.12 (a) and 20.12A). In such circumstances, where Clause 20.6 (d) (iii) applies, the DMCT EPCL Report shall not be produced until the relevant final DMCT Testing Report or other test completion reports on which it relies have been produced.

20.42 The DCC may combine the activities described in Clause 20.41 so that a single DMCT EPCL Report may cover more than one planned entry on the EPCL.

20.43 The DCC shall publish each DMCT EPCL Report (which shall be anonymised and redacted where appropriate by the DCC) on the DCC Website and shall notify the Panel, the Secretary of State, the Authority and SEC Parties of the publication of the report.

21 SMETS1 Uplift Testing

21.1 Only Clauses 1, 2 and 16 of this SMETS1 SVTAD shall apply to SMETS1 Uplift Testing, unless expressly stated in the relevant SMETS1 Uplift DCC Testing Approach Document or SMETS1 Uplift Mandated User Testing Document.

21.2 SMETS1 Uplift Testing shall be performed by the DCC and any other Party that participates in it in accordance with Good Industry Practice. The DCC may overlap SMETS1 Uplift Testing if provided for in the relevant SMETS1 Uplift DCC Testing Approach Document(s) and/or SMETS1 Uplift Mandated User Testing Document(s).

21.2A Clauses 21.3 to 21.6 and Clauses 21.11 to 21.13 shall apply in respect of each SMETS1 Uplift where the SMETS1 Uplift DCC Test Approach Document has been approved by the TAG (pursuant to Clause 21.4) prior to 22 September 2021. For the avoidance of doubt, Clauses 21.1 to 21.2 and Clauses 21.7 to 21.10 shall apply in respect of each SMETS1 Uplift.

21.2B Where the SMETS1 Uplift DCC Test Approach Document has not been approved by the TAG (pursuant to Clause 21.4) prior to 22 September 2021 or where the TAG agrees to the DCC retracting any SMETS1 Uplift DCC Test Approach Document which was approved (pursuant to Clause 21.4) prior to 22 September 2021, then the DCC shall propose an approach for SMETS1 Uplift Testing for agreement by the TAG. The proposed approach shall include:

(a) the DCC's approach to testing the change (including when and where testing should be undertaken, the tests to be undertaken and the approach to regression testing), rules for test completion and the associated governance; and

(b) an indication of whether testing by Users is required.

Notwithstanding the above and for the avoidance of doubt, Clauses 21.1 to 21.2 and Clauses 21.7 to 21.10 shall apply in respect of each SMETS1 Uplift.

21.2C Where an approach for SMETS1 Uplift Testing (pursuant to Clause 21.2B) cannot be agreed by the DCC and the TAG, the matter shall be referred to the Secretary of State for determination whose decision will be final and binding for the purpose of this Code. The DCC shall undertake testing in accordance with the approach and governance as agreed with the TAG or determined by the Secretary of State (as the case may be).

21.3 Each time that a SMETS1 Uplift is planned which would require a change to the DCC Total System, the DCC shall prepare a draft SMETS1 Uplift DCC Testing Approach Document, which shall set out the DCC's proposals for SMETS1 Uplift DCC Testing including:

(a) the proposed amendments to this Code that are the subject of the testing, an explanation of the associated changes to the DCC Total System, and the testing objective;

(b) the SMETS1 Device Model and/or the combinations of SMETS1 Device Models that are to be used in testing or a statement as to why testing using Devices is not considered necessary;

(c) the testing environments to be used;

(d) the requirements (if any) for security testing;

(e) the requirements (if any) for system capacity testing;

(f) the testing that shall be undertaken, both in terms of the scope of testing and the extent of testing (including negative tests) and the approach to regression testing;

(g) the applicable Testing Issue Thresholds and the process for excluding Testing Issues;

(h) the exit criteria for testing to complete successfully;

(i) any perceived risks associated with the approach to testing and the proposed mitigations;

(j) the approach to providing for assurance of the testing undertaken; and

(k) matters to be included in the SMETS1 Uplift DCC Testing Completion Report (to be prepared pursuant to Clause 21.7).

21.4 The DCC shall submit each draft SMETS1 Uplift DCC Testing Approach Document to the TAG for review (and such submission by the DCC and review by the TAG may take place prior to this Clause 21.4 coming into effect):

(a) where the TAG and the DCC can reach an agreement, the relevant draft SMETS1 Uplift DCC Testing Approach Document shall be updated by the DCC as necessary and deemed to be final; or

(b) where the TAG and the DCC cannot reach an agreement, the relevant SMETS1 Uplift DCC Testing Approach Document shall be referred by the DCC to the Secretary of State for determination (whose decision shall be final and binding for the purposes of this Code) and the relevant draft SMETS1 Uplift DCC Testing Approach Document shall be updated by the DCC as necessary and deemed to be final.

21.5 The DCC shall take all reasonable steps to complete the tests set out in each SMETS1 Uplift DCC Testing Approach Document in accordance with the milestone plan published by the DCC for the relevant SMETS1 Uplift DCC Testing.

21.6 Revisions to a SMETS1 Uplift DCC Testing Approach Document finalised pursuant to Clause 21.4 may, from time to time be submitted by the DCC to the TAG for agreement in accordance with the provisions of Clause 21.4, and the provisions of Clause 21.5 shall apply (again) to the revised version of the document.

21.7 Where the DCC considers that User testing is required as part of SMETS1 Uplift Testing it shall set out its proposals for User testing in a draft SMETS1 Uplift Mandated User Testing Document, including those Users that should be required to participate in the testing, the approach to testing, the arrangements for test completion and notification of test completion. In developing a SMETS1 Uplift Mandated User Testing Document, the DCC shall consult with the TAG, Parties and other relevant stakeholders prior to the submission of the document to the Secretary of State.

21.8 The DCC shall submit each draft SMETS1 Uplift Mandated User Testing Document to the Secretary of State, indicating:

(a) why the DCC considers the draft to be fit for purpose;

(b) copies of the consultation responses received; and

(c) any areas of disagreement that arose during the consultation process and that have not been resolved.

21.9 The DCC shall comply with any direction given by the Secretary of State to re-consider, re-consult, and/or re-submit the draft document.

21.10 Should a SMETS1 Uplift Mandated User Testing Document be approved by the Secretary of State, the DCC and each Party other than the DCC that participates in (or is required to participate in) testing, as set out in such approved document, shall comply with that SMETS1 Uplift Mandated User Testing Document.

21.11 Where the DCC reasonably considers that the DCC's solution testing is complete for an instance of SMETS1 Uplift DCC Testing (or a subset of the solution), the DCC shall prepare a report (being a SMETS1 Uplift DCC Testing Completion Report) as provided for in the SMETS1 Uplift DCC Testing Approach Document. The DCC shall present each SMETS1 Uplift DCC Testing Completion Report to the TAB for their acceptance or rejection. Where accepted by the TAB, a SMETS1 Uplift DCC Testing Completion Report shall be provided to the TAG for approval as follows:

(a) where the TAG approves the SMETS1 Uplift DCC Testing Completion Report (subject to the TAG and the DCC reaching an agreement regarding resolution of any issues raised by the TAG) the relevant SMETS1 Uplift DCC Testing Completion Report shall be updated by the DCC as necessary and deemed to be final; or

(b) where the TAG declines to approve the SMETS1 Uplift DCC Testing Completion Report, the DCC shall, if necessary, update the SMETS1 Uplift DCC Testing Completion Report (to reflect resolution of any issues where the DCC and the TAG reached an agreement), and the DCC shall either:

(i) refer the SMETS1 Uplift DCC Testing Completion Report to the Secretary of State for determination pursuant to Clause 21.12; or

(ii) continue with SMETS1 Uplift DCC Testing (and Clause 21.5 onwards shall apply again).

21.12 Where a referral has been made by the DCC (pursuant to Clause 21.11 (b) (i)) the determination of the Secretary of State shall be final and binding for the purposes of this Code as follows:

(a) where the Secretary of State agrees that SMETS1 Uplift DCC Testing is complete, the relevant SMETS1 Uplift DCC Testing Completion Report shall be updated by the DCC as necessary and deemed to be final; or

(b) where the Secretary of State disagrees that SMETS1 Uplift DCC Testing is complete, the DCC shall continue with SMETS1 Uplift DCC Testing (and Clause 21.5 onwards shall apply again).

21.13 The DCC shall publish each final SMETS1 Uplift DCC Testing Completion Report (which shall be anonymised and redacted where appropriate by the DCC) on the DCC Website and shall notify the Panel, the Secretary of State, the Authority and the SEC Parties of the publication of the report.

APPENDIX AL

SMETS1 Transition and Migration Approach Document

1 Introduction and General Obligations

1.1 This Appendix is the Transition and Migration Approach Document (TMAD) developed by the DCC pursuant to Section N6 of the Code.

1.2 Where directed to do so by the Secretary of State from time to time, the DCC shall develop and consult upon a further draft or drafts of this TMAD and submit it to the Secretary of State in accordance with the process set out in Section N6.4 of the Code.

1.3 For the purposes of Section N6.8 (Expiry of Transition and Migration Approach Document) this TMAD will cease to apply on 31 December 2024 (or any such later date as the Secretary of State may direct following a consultation on a proposed alternative with the Parties and the Panel).

1.4 The DCC shall develop proposals for amendments to the Code (and a proposed timing for their designation) that would enable SMETS1 Installations that comprise SMETS1 Meters that are In-Scope for Enrolment to be successfully Migrated, where the DCC considers that without such amendments, the successful Migration of those SMETS1 Installations is not likely to be possible.

1.5 Where the DCC considers that it would be technically or operationally impracticable or disproportionately costly to enable particular categories of SMETS1 Installations to be Migrated and/or particular categories of SMETS1 Smart Metering Systems to be Enrolled, rather than developing proposals pursuant to Clause 1.4, the DCC shall develop proposals for amendments to Clause 18 to prescribe those categories of SMETS1 Installations that should not be Migrated and/or those categories of SMETS1 Smart Metering Systems that should not be Enrolled together with the DCC's supporting rationale.

1.6 The DCC shall develop proposals pursuant to Clauses 1.4 and 1.5 in accordance with the following process:

(a) the DCC shall:

(i) in consultation with the Parties and such other persons as are likely to be interested, produce a draft of the proposals and, where applicable, the supporting rationale; and

(ii) in the case of proposals pursuant to Clause 1.5, concurrently advise each Responsible Supplier for a SMETS1 Smart Metering System that would be affected or would potentially be affected by the DCC proposals (to the extent to which the DCC reasonably knows) that the DCC is proposing that it should no longer be required to:

(A) undertake activities; and/or

(B) undertake a Migration,

that would enable that SMETS1 Smart Metering System to be Enrolled or provide SMETS1 Services to the SMETS1 Smart Metering System(s);

(b) where a disagreement arises with any Party or other person with regard to any proposals or rationale, the DCC shall endeavour to reach an agreed proposal/rationale with that Party or person;

(c) after completion of the process described in (a) and (b) above, the DCC shall submit to the Secretary of State a document or documents containing its proposed amendments to the Code (together with the supporting rationale), and shall when doing so also provide to the Secretary of State:

(i) a statement of the reasons why the DCC considers the proposal(s) and, where applicable, the supporting rationale, to be fit for purpose;

(ii) copies of the consultation responses received; and

(iii) a summary of any disagreements that arose during consultation and that have not been resolved by reaching an agreed proposal/rationale; and

(d) the DCC shall comply with any requirements in a direction given to it by the Secretary of State in relation to the document or documents, including:

(i) any amendments to be made to the document;

(ii) any requirement to produce and submit to the Secretary of State a further draft of the document; and

(iii) any requirement as to the process to be followed by the DCC (and the time within which that process shall be completed) prior to submitting a further such draft.

1.7 [NOT USED]

1.8 The DCC shall develop proposals pursuant to Clauses 1.4 and 1.5 in such timeframes as may be specified in directions issued by the Secretary of State from time to time for such purpose.

1.9 For the purposes of Clauses 1.4-1.6, SMETS1 Smart Meters that are In-Scope for Enrolment are those:

(a) for which the Secretary of State has concluded that the DCC is required to provide SMETS1 Services; and

(b) which are not SMETS1 Smart Meters that are the subject of an Excluded Category(ies) set out in Clause 18 (except where a direction has been issued by the Secretary of State pursuant to Clause 18.16).

2 Defined Terms and Interpretations

Term	Meaning
Active Device	Shall mean an Active Meter or Active GPF as the context requires.
Active GPF	Shall mean the SMETS1 GPF that is associated with a SMETS1 GSME that is an Active Meter.
Active Meter	Shall mean, at the relevant point in time, a SMETS1 ESME or a SMETS1 GSME in relation to which, at that point in time, the Responsible Supplier has arrangements with a SMETS1 SMSO to provide the Responsible Supplier with services in relation to that SMETS1 ESME or SMETS1 GSME.
Authenticator	Shall be the DCC, the DCO, the Commissioning Party, a Supplier Party or the S1SP when undertaking the processing required by Table5.9.
Authorised DCO SMETS1 Device Credentials	Shall mean the security related information required by the DCO for a SMETS1 Device which is provided to the DCO securely (and independently from the S1SP) and which the DCO is required to use to independently assure requests it receives from the S1SP in relation to the Device's installation or Migration.
Authorised S1SP SMETS1 Device Credentials	Shall mean the security related information required by the S1SP for a SMETS1 Device which is provided to the S1SP securely (and independently from the DCO) and which the S1SP is required to use in relation to the Device's installation or Migration.

Certificate ID	In relation to an Organisation Certificate, shall be the combination of serialNumber and Issuer X520 Common Name (with their Organisation Certificate Policy meanings) and so shall be a unique identifier for that Organisation Certificate. Thus, the identifier shall be the SMETS1 Migration Schema combination of the X509SerialNumber and X509IssuerName values. Where no Organisation Certificate is identified, it shall have the Null Certificate ID value.

Term	Meaning
CHF Identifier	Shall be the Device ID of the SMETS1 CHF associated with each SMETS1 Installation.
CHF Whitelist	In relation to a SMETS1 Installation, shall include the list of Device IDs, being IEEE media access control addresses, held on the SMETS1 CHF detailing the set of Devices which are currently authorised to communicate over the ZigBee network to which the CHF controls access. For clarity this list never includes Device IDs for a CHF or a GPF, and in the case of an ESME only includes the Device ID where that ESME communicates with the CHF using a ZigBee network. For clarity, the CHF Whitelist, for GroupIDs specified in Clauses 12, 13, 14, 15 and 16, includes, for each IEEE media access control address either (1) the UTC date-time at which the CHF last communicated with the identified Device or (2) an indication that the CHF has never communicated with the identified Device.
Commissioning Outcome File	Shall mean a file created by the Commissioning Party which complies with the requirements of Clause 6.3(d)(ii).
Commissioning Outcome File Counter	A counter of that name created and maintained pursuant to Table 5.7 to guard against replay of files processed pursuant to this TMAD.
Commissioning Party	See Clause 3.1(e).
Commissioning Party Systems	See Clause 3.1(e).
Commissioning Request	Shall mean a request from the Commissioning Party as set out in Table 6.3.
Common Validation Checks	Shall means those checks carried out pursuant to Clause 5.10.
Completion Report	means a report that is produced at completion of a Test Phase setting out evidence demonstrating how the criteria for the completion of that Test Phase have been met.
Critical Network Operator ID	In relation to an Organisation Certificate identified by a specified Certificate ID, if it has a Remote Party Role of 'networkOperator' and a keyUsage of 'digitalSignature', the Critical Network Operator ID shall be the Entity Identifier of the subject of that Certificate (all with their Organisation Certificate Policy meanings). Otherwise, the Critical Network Operator ID shall be null.
Critical Supplier ID	In relation to an Organisation Certificate identified by a specified Certificate ID, if it has a Remote Party Role of 'supplier' and a keyUsage of 'digitalSignature', the Critical Supplier ID shall be the Entity Identifier of the subject of that Organisation Certificate (all with their Organisation Certificate Policy meanings). Otherwise, the Critical Supplier ID shall be null.

Term	Meaning
Daily Migration Demand	Shall have the meaning given in Clause 4.8.
DCC's Microsoft SharePoint	A web-based collaborative platform that DCC uses to securely share and exchange information with individual Parties.
DCC Migration Systems	Shall have the meaning given in Clause 3.1(e).
DCO Public Key	Shall mean a public key produced pursuant to Clause 5.4A.
DCO Required File Set	Shall mean the set of files specified in Clauses 12, 13, 14, 15 and 16 for the relevant GroupID.
DCO Viable Installations	Shall have the meaning ascribed to that term in Clause 5.19.
Dormant Meter	Shall mean, in relation to a SMETS1 SMSO, a SMETS1 ESME or a SMETS1 GSME that is installed in respect of an Energy Consumer's premises, that: i) the relevant SMETS1 SMSO is able to remotely communicate with via a SMETS1 CHF; and ii) is not an Active Meter.
Excluded Category	Shall have the meaning given in Clause 18.
Group	Shall mean the set of SMETS Installations identified by the same GroupID on the Group Device Model Combination List.
Group Device Model Combination List	Shall mean a list of Device Model Combinations that are entries on the SMETS1 Eligible Product Combinations list and form part of the same Group.
GroupID	Shall be the unique value used by the DCC to identify a Group within the Group Device Model Combination List.
Group Specific Requirements	Shall mean the set of requirements as specified in Clauses 12, 13, 14, 15 and 16 for the relevant GroupID.
IEEE	The Institute of Electrical and Electronics Engineers.
Indicative Migration Forecasts	In relation to a Supplier Party and a SMETS1 SMSO, shall mean the forecast number of all SMETS1 Installations that the Supplier Party is planning to include within a Migration Authorisation each day and the associated dates. This forecast shall be broken down by Electricity Network Party.
Installing Supplier	Means, in relation to a Device, the Supplier Party that installed, or arranged for the installation of, that Device.

Term	Meaning
Key Identifier	The SHA-1 hash of a Public Key that is used to identify that Public Key, where SHA-1 has the meaning specified in the US Government's Federal Information Processing Standards document 180-4.
Last EPCL Entry	Means, in respect of entries that include Secure SMSO Limited (company number 10611361) or, with effect from the novation of the enduring SMETS1 agreement between DCC and Secure SMSO Limited, its transferee, Secure Meters (UK) Limited (company number 02199653), the entry on the list of SMETS1 Eligible Product Combinations which has been approved by the Secretary of State after which no other entries in respect of Secure SMSO Limited have been approved by the Secretary of State for a period of 12 months.
Migration	Shall have the meaning given in Clause 3.1(e).
Migration Authorisation	An authorisation given by the Responsible Supplier in relation to a SMETS1 Installation via the Migration Authorisation Mechanism to commence the Migration of a SMETS1 Installation, or an authorisation deemed to be given in accordance with Clause 4.27. Except where GroupID = "EA" or "EB", where there are two Responsible Suppliers for the Smart Metering Systems that together comprise the same SMETS1 Installation and they are Affiliates of one another, then any authorisation for the Migration of the SMETS1 Installation from the Responsible Supplier for the Electricity Smart Metering System shall, where the Migration Authorisation Mechanism also includes details of the Gas Smart Metering System, be deemed to constitute an authorisation for Migration of the SMETS1 Installation by the Responsible Supplier for the Gas Smart Metering System.
Migration Authorisation Mechanism	The mechanism of that name referred to in Clause 4.35.
Migration Common File	Shall mean a file created by a Requesting Party pursuant to Clause 5.8 that details information about SMETS1 Installations, along with the additional requirements for the relevant GroupID.
Migration Common File Counter	A counter of that name created and maintained pursuant to Table 5.7 to guard against replay of relevant files processed pursuant to this TMAD.
Migration Common Validation File	Shall mean a file created by the DCC pursuant to Clause 5.10(b) detailing, for a corresponding Migration Common File, which SMETS1 Installations have passed the Common Validation Checks and which have not. For those which have not, the file shall specify the validation failure. For clarity, any SMETS1 Installation which does not pass the Common Validation Checks shall not be further processed by the DCC in relation to the corresponding Migration Common File.
Migration Common Validation File Counter	A counter of that name created and maintained pursuant to Table 5.7 to guard against replay of relevant files processed pursuant to this TMAD.

Term	Meaning
Migration Demand Commitment	Shall have the meaning given in Clause 4.8(b).
Migration Error Handling and Retry Strategy	Shall have the meaning set out in Clause 8.8.
Migration Group Encrypted File	Shall mean a file created by a Requesting Party pursuant to Clause 5.12(g) which details a list of SMETS1 Installations which the Requesting Party wishes to Migrate, as identified by the CHF Identifier of each, along with the additional Group Specific Requirements for the relevant GroupID. For clarity, such files shall only be processed where they are specified as being required in Group Specific Requirements.
Migration Group Encrypted File Counter	A counter of that name created and maintained pursuant to Table 5.7 to guard against replay of relevant files processed pursuant to this TMAD.
Migration Group File	Shall mean a file created by a Requesting Party pursuant to Clause 5.12(f) which details a list of SMETS1 Installations which the Requesting Party wishes to Migrate as identified by the CHF Identifier of each, along with, where required for the Group identified by GroupID, any additional Group Specific Requirements for the relevant GroupID. For clarity, such files shall only be processed where they are specified as being required in the Group Specific Requirements.
Migration Group File Counter	A counter of that name created and maintained pursuant to Table 5.7 to guard against replay of relevant files processed pursuant to this TMAD.
Migration Header	In relation to a file created pursuant to this TMAD, the combination of the values in the RequestingPartyID and MCFCounter elements, each with the meaning set out in Clause 10.
Migration Incident	Shall have the meaning given in Clause 3.1(e).
Migration Reporting Regime	Shall have the meaning given in Clause 4.45.
Migration Scaling Methodology	Shall have the meaning given in Clause 4.11
Migration Week	Means in relation to a SMETS1 SMSO, a period of seven days commencing on a Monday and within which DCC plans to Migrate one or more SMETS1 Installations that pertain to that SMETS1 SMSO, although it is acknowledged that, in the case of Group ID = “EA” or “EB”, the Migration might not complete within that week. The first Migration Week for a SMETS1 SMSO shall commence on the first Monday following the day on which an entry for a combination of Device Models which lists that SMETS1 SMSO, as part of that entry, has been added to the SMETS1 Eligible Product Combinations.

Term	Meaning
Network Operator Certificate ID	The Certificate ID of an Organisation Certificate that has been Issued to a Network Party.
Non-Critical Network Operator ID	In relation to an Organisation Certificate identified by a specified Certificate ID, if it has a Remote Party Role of 'networkOperator' and a keyUsage of 'keyAgreement', the Non-Critical Network Operator ID shall be the Entity Identifier of the subject of that Certificate (all with their Organisation Certificate Policy meanings). Otherwise, the Non-Critical Network Operator ID shall be null.
Non-Critical Supplier ID	In relation to an Organisation Certificate identified by a specified Certificate ID, if it has a Remote Party Role of 'supplier' and a keyUsage of 'keyAgreement', the Non-Critical Supplier ID shall be the Entity Identifier of the subject of that Certificate (all with their Organisation Certificate Policy meanings). Otherwise, the Non-Critical Supplier ID shall be null.
Null Certificate ID	Shall be the Certificate ID used to mean that no Certificate is identified. The value of Null Certificate ID shall be the combination where serialNumber and Issuer X520 Common Name (with their Organisation Certificate Policy meanings) are '0' and 'NULL' respectively.
Plaintext	When used in relation to symmetric key encryption / decryption, shall have its GBCS meaning. When used in relation to public key encryption / decryption, shall mean the 'message M' with its IETF RFC-8017 meaning.
Recently Dormant SMETS1 Installation	means a SMETS1 Installation that: (a) comprises a Device Model Combination that is eligible to be Enrolled; (b) included one or more Active Meters at any point in time after it became eligible to be Enrolled; and (c) at a point in time after 12 November 2020, became a SMETS1 Installation that comprises only Dormant Meter(s).
Recovery Time Objective	Shall be the targeted duration of time within which a system must be restored after a disaster (or disruption).
Recovery Point Objective	Shall be the targeted duration of time over which Data can be lost due to a Major Incident.

Term	Meaning
Relevant Device	Means an Active Meter in a SMETS1 Installation with which, prior to the UTRN Period, Secure SMSO Limited (company number 10611361) or, with effect from the novation of the enduring SMETS1 agreement between DCC and Secure SMSO Limited, its transferee, Secure Meters (UK) Limited (company number 02199653) communicated on behalf of the Responsible Supplier.
Request to Exclude	A list of MPRN(s) and associated Device ID(s) provided pursuant to Clause 5.8C and in the format specified in Clause 5.8D.
Requested Installations	Shall have the meaning ascribed to that term in Clause 5.12.
Requesting Party	See Clause 3.1(e).
Requesting Party Systems	See Clause 3.1(e).
RP Decommissioning Date	Means, in relation to a Requesting Party, the decommissioning date identified in relation to that Requesting Party in a RP Decommissioning Timetable.
RP Decommissioning Timetable	The timetable of that name for each Requesting Party most recently approved by the Secretary of State pursuant to Clause 7.3.
Single Use Authorisation Code (SUA)	A one-time authorisation code used by Devices with GroupID = “DA” when cryptographically verifying Instruction.
S1SP Commissioning File	Shall mean a file created by the S1SP pursuant to Clause 5.27(c)(ii) which details whether, for the SMETS1 Installations in question, the S1SP successfully undertook the processing required of the S1SP and, if not fully successful, the issues arising in that processing.
S1SP Commissioning File Counter	A counter of that name created and maintained pursuant to Table 5.7 to guard against replay of files processed pursuant to this TMAD.
S1SP Required File Set	Shall mean the set of files specified for the relevant GroupID.
S1SP Viable Installations	Shall have the meaning set out in Clause 5.25.
SMETS1 CAD	Shall be a Device operating on a home area network created by a SMETS1 CHF, which is not a SMETS1 ESME, a SMETS1 GSME, a SMETS1 CHF, a SMETS1 GPF, a SMETS1 PPMID or a SMETS1 IHD.
SMETS1 Device Security Testing	means tests carried out by the DCC in accordance with the requirements of Clause 17.
SMETS1 Device Security Testing Completion Report	means the document of that name developed pursuant to Clause 17.11.

Term	Meaning
SMETS1 Device Security Testing Scope and Timetable Document	means the document of that name developed pursuant to Clause 17.3.
SMETS1 Installation	Means a SMETS1 CHF installed in respect of an Energy Consumer's premises, the SMETS1 GPF which is part of the same SMETS1 CH, the SMETS1 ESME with which the SMETS1 CHF can communicate, and the set of other Devices (if any) which are authorised to communicate over the HAN to which the CHF controls access. The set of other Devices within a SMETS1 Installation shall include at most one SMETS1 GSME, at most one SMETS1 PPMID, at most one SMETS1 IHD and at most one SMETS1 CAD.
SMETS1 Loss of System Availability	Shall have the meaning given in Clause 3.1(e).
SMETS1 Migration Interface	Shall be the technical interface, as specified at Clause 9, used for the exchange of files between the DCC and Supplier Parties pursuant to the requirements to exchange files in this TMAD.
SMETS1 Migration Schema	The XML SMETS1 Migration Schema included at Clause 10.
SUA Symmetric Key	A secret, symmetric key used by the DCO to authorise Critical Instructions (with its SMETS1 Supporting Requirements meaning), in relation to Devices with a GroupID = "DA".
Supplier Certificate ID	The Certificate ID of an Organisation Certificate that has been Issued to a Supplier Party.
Supplier Signifier	The Party Signifier of the Supplier Party identified by the Entity Identifier of the subject in the Organisation Certificate identified by any CriticalSupplierCertificateID in the Migration Common File. If any CriticalSupplierCertificateID in the Migration Common File is the Null Certificate ID, the value of the Supplier Signifier shall be the empty string.
UTRN Period	In relation to an ESME or a GSME that forms part of a SMETS1 Installation that is within the Group with a GroupID = "DA", a period that: (a) commences from the time at which the step in 3.14C(a) has been successfully passed in relation to that Device; and (b) has a duration that is 336 hours.

2.2 The XML elements listed in Table 10.1 are references to the parts of the SMETS1 Migration Schema and shall have the meaning given to them in the SMETS1 Migration Schema. Where such XML elements are referred to in this TMAD, then as the context requires, the reference shall be interpreted to be either to the element that is to be populated or to the information that is populated within that element for a particular file.

2.3 Additionally, where defined terms from specific parts of the Code are used, the relevant part of the Code is stated. Where no specific part of the Code is stated, a defined term shall have its Section A (Definitions and Interpretation) meaning.

2.4 Where this TMAD affords rights to, or imposes obligations on, a Party in relation to a Migration Week, then, until such time as an entry exists on the list of Eligible Product Combinations in respect of a particular SMSO, the term "Migration Week" in respect of that SMSO shall be interpreted as meaning each week that the Party reasonably anticipates will be a Migration Week (based on the milestones set out in the SMETS1 Services delivery plan produced pursuant to condition 13 of the DCC Licence).

3 Transitional Application of Sections of the Code

Application of Section A (Definitions and Interpretation)

3.1 Whilst this TMAD remains in force, Section A (Definitions and Interpretation) of the Code shall apply as follows:

(a) the definition of "DCC Live Systems" shall be replaced with the following:

DCC Live Systems means those parts of the DCC Total System which are used for the purposes of:

(a) (other than to the extent to which the activities fall within paragraph (b), (c), (f), (g), (h), (i), (j), (k) or (l) below) processing (including Countersigning of SMETS1 Responses, SMETS1 Alerts and S1SP Alerts, but not Countersigning of SMETS1 Service Requests) Service Requests, Pre-Commands, Commands, Instructions, Service Responses and Alerts, holding or using Registration Data for the purposes of processing Service Requests and Signed Pre-Commands, and providing the Repository Service;

(b) Threshold Anomaly Detection (other than that carried out by a DCO) and (other than to the extent to which the activity falls within paragraph (d), (f), (g), (h), (i), (j), (k) or (l) below) Cryptographic Processing relating to the generation and use of a Message Authentication Code and Countersigning SMETS1 Service Requests;

(c) discharging the obligations placed on the DCC in its capacity as CoS Party;

(d) providing SMKI Services;

(e) the Self-Service Interface;

(f) discharging the DCC's obligations under the SMKI Recovery Procedure;

(g) the Production Proving Systems;

(h) discharging the obligations of any SMETS1 Service Provider in its capacity as such;

(i) discharging the obligations of any DCO in its capacity as such;

(j) discharging the obligations of the CSS Provider in its capacity as such;

(k) discharging the obligations of any Requesting Party in its capacity as such; and

(l) discharging the obligations of the Commissioning Party in its capacity as such.

(b) the definition of "DCC Individual Live System" shall be replaced with the following:

DCC Individual Live System

means, with regard to the DCC's duty to Separate parts of the DCC Total System, a part of the DCC Total System which is used:

(a) for one of the purposes specified in paragraphs (a) to (g), or (j) or paragraph (l) of the definition of DCC Live Systems, where the part used for each such purpose shall be treated as an individual System distinct from:

(i) the part used for each other such purpose; and

(ii) any part used for a purpose specified in either paragraphs (h) to (k) of the definition of DCC Live Systems; or

(b) by a SMETS1 Service Provider for the purpose specified in paragraph (h) of the definition of DCC Live Systems, where the part used by each

SMETS1 Service Provider shall be treated as an individual System distinct from:

(i) the part used by each other SMETS1 Service Provider; and

(ii) any part used for a purpose specified in any of paragraphs (a) to (g), or paragraphs (i) to (l), of the definition of DCC Live Systems; or

(c) by a DCO for the purpose specified in paragraph (i) of the definition of DCC Live Systems, where the part used by each DCO shall be treated as an individual System distinct from:

(i) the part used by each other DCO; and

(ii) any part used for a purpose specified in any of paragraphs (a) to (h) or paragraphs (j) to (l) of the definition of DCC Live Systems; or

(d) by a Requesting Party for the purpose specified in paragraph (k) of the definition of DCC Live Systems, where the part used by each Requesting Party shall be treated as an individual System distinct from:

(i) the part used by each other Requesting Party; and

(ii) any part used for the purpose specified in any of paragraphs (a) to (j) or paragraph (l) of the definition of DCC Live Systems.

(c) the definition of "Planned Maintenance" shall be replaced with the following:

Planned Maintenance means, in respect of a month, Maintenance of the DCC Systems planned prior to the start of that month or, in the case of DCC Migration Systems, planned 10 Working Days prior to the start of the Maintenance, and which will disrupt, or poses a Material Risk of disruption to, the provision of the services.

(d) The definition of "Responsible Supplier" shall be replaced with the following:

Responsible Supplier means in respect of a Smart Metering System (or any Device forming, or intended to form, part of a Smart Metering System) or a SMETS1 Installation (or any Device forming part of a SMETS1 Installation) which relates to:

(a) an MPAN, the Import Supplier for the Electricity Meter that forms part of that Smart Metering System or SMETS1 Installation; and/or

(b) an MPRN, the Gas Supplier for the Gas Meter that forms part of that Smart Metering System or SMETS1 Installation.

(e) the following definitions shall be added to Section A:

Commissioning Party	Shall mean the DCC when performing the tasks ascribed to the Commissioning Party in this Code.
Commissioning Party Systems	That part of the DCC Total System used for the purposes referred to in sub-paragraph (l) of the definition of DCC Live Systems.
DCC Migration Systems	Shall mean the Requesting Party Systems and the Commissioning Party Systems.
Migration	In relation to a SMETS1 Installation, or any Device comprising part of that SMETS1 Installation, the carrying out of each of the steps (where relevant to the point of failure) set out in Clauses 5 and 6 of the Transition and Migration Approach Document in relation to that SMETS1 Installation or Device; and the term "Migrate" shall be interpreted accordingly.
Migration Incident	Shall mean an Incident that relates to the Services provided pursuant to the Transition and Migration Approach Document.
Requesting Party	Shall mean, in relation to each of one or more Groups, the DCC when performing the tasks ascribed to the Requesting Party in this Code.
Requesting Party Systems	Shall mean those parts of the DCC Total System used when carrying out the role of a Requesting Party, provided that any SMETS1 SMSO's Systems from which information is provided to the Requesting Party for the purposes of populating the content of any Migration Common File, Migration Group File or Migration Group Encrypted File (each as defined in the Transition and Migration Approach Document) shall not be considered to form part of the Requesting Party Systems.

Smart Metering Inventory Systems	Shall mean that part of DCC Systems that is capable of adding to, modifying or removing any information held in the Smart Metering Inventory and any other part of DCC Systems that is not Separated from it.
SMETS1 Loss of System Availability	Shall mean a material loss of availability, other than for Maintenance purposes, of the DCC Migration Systems, or any of its individual components.

(f) an additional rule of interpretation shall apply such that words beginning with capital letters which are defined in this TMAD and used elsewhere in this Code shall, unless the context otherwise requires, have the meanings given to them in this TMAD; and

(g) the definitions set out below shall be added to Section A or, where they already exist in Section A, they shall be replaced with the meanings set out below:

Application Association	has the meaning given to that expression in the DLMS COSEM Green Book (DLMS UA 1000-2 Ed. 8), published by the DLMS User Association.
Authentication Key	has the meaning given to that expression in the DLMS COSEM Green Book (DLMS UA 1000-2 Ed. 8), published by the DLMS User Association.
Cryptographic Processing	means the generation, storage (other than of Secret Key Material used in relation to communications with a SMETS1 Device, where that Secret Key Material is encrypted) or use of any Secret Key Material.
Instruction	means, in respect of a SMETS1 Device, a communication generated by the SMETS1 Service Provider or a DCO following receipt of a SMETS1 Service Request by the DCC that is designed to instruct the Device to execute the functionality necessary to permit the DCC to take the necessary Equivalent Steps.
SMETS1 PPMID	means: (a) where GroupID = “EA” or “EB”, a SMETS1 IHD that is capable of upgrading its Firmware in response to an Instruction sent over the SMETS1 SM WAN; or

	(b) except where GroupID = "EA" or "EB", a SMETS1 IHD that is capable of upgrading its Firmware in response to an Instruction sent over the SMETS1 SM WAN (except such Devices where, during assessment by the DCC under the DMCT Process (pursuant to Clause 20.4 and 20.5 of Appendix AK), the DCC is unable to obtain from either the Supplier Party or the SMETS1 SMSO the set of data for the SMETS1 PPMID Device Model that is required to enable the relevant entry to be made as a SMETS1 PPMID on the list of SMETS1 Eligible Product Combinations).
SMETS1 Symmetric Key	means an Authentication Key or a symmetric key which is in either case used to process communications with SMETS1 Devices.
Transport Layer Security	means in accordance with the relevant SMKI PMA and SSC Guidance (Standards, Procedures and Guidelines) published on the SEC website.

3.1 ANo SMETS1 SMSO Systems (other than to the extent they are used to carry out Requesting Party activities) shall be considered to form part of the DCC Total System for the purposes of this Code.

Application of Appendix AC (Inventory Enrolment and Decommissioning Procedures)

3.2 The provisions of Clauses 3.4 and 3.5 of the Inventory Enrolment and Decommissioning Procedures shall not apply to the addition of SMETS1 Devices to the Smart Metering Inventory where those Devices form part of a SMETS1 Installation that is to be Migrated.

3.3 For the purposes of Migration, SMETS1 Devices may be added to the Smart Metering Inventory by the following organisations:

(a) in the case of a SMETS1 CHF, an S1SP; or

(b) in the case of any other SMETS1 Device, the Responsible Supplier for the Device or the Commissioning Party but, in either case, only in circumstances where the Device forms part of a SMETS1 Installation that is identified within a SMETS1 Commissioning File as having completed all the checks and processing referred to in Clause 5.27 without any failures flagged as ‘Critical’.

Application of Appendix AG (Incident Management Policy)

3.4 Whilst this TMAD remains in force, Appendix AG shall be modified as follows:

(a) The definition of Live Services shall be replaced with the following definition:

Live Services	Means: (a) any of the Services that the DCC is obliged to provide to a User, an Authorised Subscriber, a DCC Gateway Party (once its connection is capable of operation), but excluding Testing Services; (b) the exchange of data pursuant to Section E2; and (c) any of the Services provided pursuant to the TMAD.

3.5 The provisions of the Incident Management Policy shall apply to Migration Incidents provided that the following variations shall apply:

(a) Clause 2.1.3 of Appendix AG shall not apply in respect to Migration Incidents;

(b) Clause 5.2 of Appendix AG shall not apply in respect of DCC Migration Systems;

(c) where the DCC ought to be reasonably able to resolve a Migration Incident without the assistance of any Responsible Supplier, or the DCC ought to be able to arrange for the relevant SMETS1 SMSO to do so without the assistance of any Responsible Supplier, any incident resolution activities associated with a Migration Incident shall be assigned to the DCC; otherwise the incident resolution activities shall be assigned to the Responsible Supplier;

(d) except where an Incident is required to be raised by the DCC pursuant to this TMAD, the DCC shall not be required to raise an Incident, and no Party shall have the right to raise an Incident, in circumstances where a Responsible Supplier or the SMETS1 SMSO is notified by the DCC in accordance with this TMAD that one or more of the steps in the Migration of a SMETS1 Installation have not been successfully completed; and

(e) Table 1 in Clause 2.4 of Appendix AG shall be replaced with the following Table:

Incident Category	**Description**	**Target Initial Response Time**	**Target Resolution Time**
1	A Category 1 Incident (Major Incident) is an Incident which, in the reasonable opinion of the DCC: • prevents a large group of Incident Parties from using the Live Services; • has a critical adverse impact on the activities of the Incident Parties using the Live Services of the DCC; • has a critical adverse impact on the activities necessary to Migrate SMETS1 Installations comprising Dormant Meters pursuant to the Transition and Migration Approach Document; • causes significant financial loss and/or disruption to the Incident Parties; or • results in any material loss or corruption of DCC Data. For a Major Security Incident there are additional considerations: • HMG, through CPNI, have declared a Major Incident based on their procedures; • a pattern has been seen across the DCC Total System that in total would have a significant security impact; or • Data covered by the Data Protection Act has either been lost or obtained by an unauthorised party, or is seriously threatened.	10 minutes	4 hours

2	An Incident which in the reasonable opinion of the DCC: • has a non-critical adverse impact on the activities of Incident Parties, but the Live Service is still working at a reduced capacity; • causes financial loss and/or disruption to other Incident Parties which is more than trivial but less severe than the significant financial loss described in the definition of a Category 1 Incident; or • has a non-critical adverse impact on the activities necessary to Migrate SMETS1 Installations comprising Dormant Meters pursuant to the Transition and Migration Approach Document.	20 minutes	24 hours
3	An Incident which, in the reasonable opinion of the DCC: • has an adverse impact on the activities of an Incident Party but which can be reduced to a moderate adverse impact due to the availability of a workaround; • has a moderate adverse impact on the activities of an Incident Party; or • has a moderate adverse impact on the activities necessary to Migrate SMETS1 Installations comprising Dormant Meters pursuant to the Transition and Migration Approach Document.	45 minutes	72 hours
4	An Incident which, in the reasonable opinion of the DCC: • has a minor adverse impact on the activities of an Incident Party; or • has a minor adverse impact on the activities necessary to Migrate SMETS1 Installations comprising Dormant Meters pursuant to the Transition and Migration Approach Document.	3 hours	5 days

5	An Incident which, in the reasonable opinion of the DCC: • has minimal impact on the activities of Incident Party; or • has minimal impact on the activities necessary to Migrate SMETS1 Installations comprising Dormant Meters pursuant to the Transition and Migration	1 day	10 days

Application of Section F (Smart Metering System Requirements)

3.6 Whilst this TMAD remains in force, for the purposes of Section F2.10A (SMETS1 Lists), each entry that is made on each of the SMETS1 Pending Product Combinations and SMETS1 Eligible Products Combinations lists shall, in addition to setting out a combination of Device Models and communication services provider, additionally include, in relation to that entry, the identity of the SMETS1 SMSO, and whether that entry applies to SMETS1 Installations comprising either (i) solely Dormant Meters (ii) solely Active Meters; or (iii) either Dormant Meters and/or Active Meters. However, the requirement to identify the aforementioned additional information shall not apply to any entry on the SMETS1 Pending Product Combinations or SMETS1 Eligible Products Combinations lists that is made whilst this TMAD remains in force but after the expiry of the RP Decommissioning Date for the Requesting Party that formed part of the SMETS1 SMSO that would otherwise have appeared in that entry. Where either list contains two or more entries that have the same combination of Device Models but identify different SMETS1 SMSOs and/or different permitted combinations of Active Meters / Dormant Meters, each entry shall be treated as a separate entry for the purpose of the list and the requirements of Section H5.8 shall be modified accordingly so that the words “listed on the SMETS1 Eligible Product Combinations” (in both places that they appear) are replaced with “which match all of the characteristics of an entry on the SMETS1 Eligible Product Combinations”. The requirements of Section H5.9 shall be modified so that the words “that is listed on the SMETS1 Eligible Products Combinations” are replaced with “which match all of the characteristics of an entry on the SMETS1 Eligible Product Combinations”.

3.7 With the exception of those that arise as a consequence of SMETS1 Pending Product Combination Tests, the DCC shall not add an entry to the list of SMETS1 Eligible Product Combinations other than to the extent that it has the approval of the Secretary of State to do so. In the case of a manifest error in the submission, approval and / or addition of an entry to the list of SMETS1 Eligible Product Combinations the Secretary of State may take such steps as are reasonably necessary to correct for such error(s) and / or direct the DCC to take such steps as are reasonably necessary to correct the error(s). The DCC shall promptly notify all SEC Parties, the Panel, the Authority and the Secretary of State where steps are taken to correct errors pursuant to this Clause 3.7.

Application of Section G (Security)

3.8 For the purposes of Section G (with the exception of Sections G2.19 to G2.24 inclusive), no Requesting Party Systems shall be considered to form part of the DCC Total System; provided that the DCC shall ensure that the requirements of Clause 11 are met in relation to each Requesting Party and each associated SMETS1 SMSO.

3.9 The Commissioning Party Systems shall not be considered to form part of the DCC Live Systems for the purposes of Sections G2.23, G2.25, G3.13 or G3.14.

3.10 Whilst this TMAD remains in force, the following additional requirement shall apply under Section G4 (Organisational Security: Obligations on Users and the DCC): The DCC shall ensure that no individual is engaged in:

(a) the development of bespoke software or firmware, or the customisation of any software or firmware, for the purpose of its installation on any part of the Commissioning Party Systems; or

(b) the development, design, build, testing, configuration, implementation, operation, maintenance, modification or decommissioning of any part of the Commissioning Party Systems,

unless that individual satisfies the requirements of Clause 3.11.

3.11 An individual satisfies the requirements of this Clause only if, at any time at which that individual is engaged in any activity described in Clause 3.10, he or she:

(a) is not at the same time also engaged in:

(i) the development of bespoke software or firmware, or the customisation of any software or firmware, for the purpose of its installation on any Smart Metering Inventory Systems; or

(ii) the development, design, build, testing, configuration, implementation, operation, maintenance, modification or decommissioning of any Smart Metering Inventory

Systems; and

(b) has not been engaged in any activity described in paragraph (a) for a period of time which the DCC reasonably considers to be appropriate, having regard to the need to ensure the management of risk in accordance with the DCC Information Security Management System.

3.12 Whilst this TMAD remains in force, the following additional requirement shall apply under Section G2 (System Security: Obligations on the DCC):

(a) The DCC shall ensure that no resources which form part of the Commissioning Party Systems also form part of its Smart Metering Inventory Systems.

3.13 The Commissioning Party Systems do not need to comply with the requirements of Section G (Security) which apply to User Systems or which apply to RDP Systems (via Section E (Registration Data)); save that Section G6 (Anomaly Detection Thresholds: Obligations on the DCC and Users) shall apply to the Commissioning Party as if it was a User.

3.14 The DCC shall ensure that Anomaly Detection Thresholds set in relation to the Commissioning Party are 0 for all requests that are not Commissioning Requests.

3.14A [NOT USED]

3.14B For GroupID = “DA”, the DCC shall, in relation to each Relevant Device during the UTRN Period for that Device, ensure that any request to generate a SMETS1 UTRN for a non-negative prepayment top-up in relation to that Device that;

(a) is received by the SMETS1 SMSO; and

(b) had it been received prior to the commencement of the UTRN Period, would have been processed by the SMETS1 SMSO,

is processed by the SMETS1 SMSO and/or the SMETS1 Service Provider (as the case may be) in materially the same manner (including to have the same effect on the Relevant Device) as it would have had, if it had been processed by the SMETS1 SMSO prior to the commencement of the UTRN Period.

3.14C The DCC shall ensure that the SMETS1 SMSO for GroupID = “DA”:

(a) is not capable of generating a SMETS1 UTRN in relation to a SMETS1 Device after the S1SP has successfully processed a Service Request with Service Reference Variant 8.1.1 for that SMETS1 Device as set out in Clause 8.1 and Table 8.7.2; and

(b) does not provide any response to a request to generate a SMETS1 UTRN in relation to such a SMETS1 Device after the step in Clause 3.14C(a), other than a response that is generated by the relevant S1SP in accordance with Clause 3.14D below.

3.14D For GroupID = "DA":

(a) during the UTRN Period for an ESME or GSME and where the S1SP receives a request to generate a SMETS1 UTRN for such a SMETS1 Device from the SMETS1 SMSO, the S1SP shall send a UTRN for the Relevant Device, that is consistent with the request, to that Device and / or to that SMETS1 SMSO; and

(b) after the UTRN Period ends for the Relevant Device, shall only send a response to the SMETS1 SMSO that indicates that the request to generate a UTRN has been unsuccessful.

3.14E The DCC shall ensure that, by no later than 15 months after the Last EPCL Entry for the S1SP related to the GroupID = "DA", all interfaces to the Systems of that S1SP that are not required by the DCC for the provision of Services under this Code (excluding any amendments to those Services made by virtue of this TMAD) are securely and irrevocably disconnected from the Systems of the S1SP.

3.14F The DCC shall as soon as reasonably practicable following the carrying out of the steps referred to in Clause 3.14E, obtain an independent audit and provide to the SMKI PMA and the Security Sub-Committee the report of that audit confirming that the steps have been properly and successfully carried out together with any remediation plan that may be required.

Application of Section H (DCC Services)

3.15 Whilst this TMAD remains in force:

(a) [Not used];

(b) Section H8.3(b) (Maintenance of the DCC Systems) shall not apply in respect of the DCC Migration Systems. The DCC may undertake Planned Maintenance of the DCC Migration Systems at any time during any day, provided that the DCC shall only undertake such maintenance when it is not likely to have an adverse impact on the ability to Migrate the number of SMETS1 Installations that the DCC has committed to Migrate on that day;

(c) Section H8.4 (Maintenance of the DCC Systems) shall be modified in respect of DCC Migration Systems, such that no later than 10 Working Days prior to the start of Planned Maintenance on the DCC's Migration Systems, the DCC makes available to Parties, to Registration Data Providers and to the Technical Architecture and Business Architecture Sub-Committee a schedule of that maintenance. Such schedule shall set out (as a minimum) the following:

(i) the proposed Maintenance activity (in reasonable detail);

(ii) the parts of the Services that will be disrupted (or in respect of which there is a Material Risk of disruption) during each such Maintenance activity;

(iii) the time and duration of each such Maintenance activity; and

(iv) any associated risk that may subsequently affect the return of normal Services.

(d) Section H8.5 shall be modified such that it also applies in respect of the schedule made available pursuant to Clause 3.15(c).

(e) Section H10.13 (Business Continuity and Disaster Recovery Targets) shall not apply in respect of a SMETS1 Loss of System Availability. Instead, the DCC shall:

(i) take all reasonable steps to ensure that the Services supported by the DCC Migration Systems are restored in accordance with the following Target Service Levels, and in any event shall ensure that the Services supported by the DCC Migration Systems are restored in accordance with the following Minimum Service Levels; and

	Target Service level	**Minimum Service Level**
Recovery Time Objective	4 hours	8 hours
Recovery Point Objective	15 minutes	30 minutes

(ii) within 21 Working Days of a SMETS1 Loss of System Availability which is not deemed to be a Major Incident, produce a report setting out:

(A) the nature, cause and impact of that SMETS1 Loss of System Availability;

(B) the action that was taken to resolve the SMETS1 Loss of System Availability;

(C) any failure to achieve the Target Service Level and/or the Minimum Service Level for the Recovery Time Objective and/or the Recovery Point Objective;

(D) whether there is likely to be a reduction in DCC External Costs as a result of any failure to meet the Target Service Level(s) and/or Minimum Service Level(s); and

(E) the steps the DCC is taking to prevent re-occurrence or continuation of that reason for the SMETS1 Loss of System Availability.

(f) The DCC shall make the report under Clause 3.15(e) available to the SEC Panel. The SEC Panel shall make the report available to Parties subject to any redactions it considers necessary to avoid a risk of Compromise to the DCC Total System, User Systems, RDP Systems and/or Devices.

(g) Section H5.8 of the Code shall be modified in accordance with the provisions of Clause 3.6 of TMAD. Where there is any conflict between Sections H5.8 to H5.9 of the Code and Clause 18 of this TMAD, Clause 18 of this TMAD shall take precedence.

Application of Section L (Smart Metering Key Infrastructure and DCC Key Infrastructure)

3.16 Whilst this TMAD remains in force, each of the rows in the table in Section L3.18 (Organisation Certificates) as modified by the provisions of Clause 3.1(d) of Appendix AS (ECoS Transition and Migration Approach Document) that correspond to the "Remote Party Role" identified in the following table shall be replaced with the corresponding rows in the following Table:

Remote Party Role	**Party**	**User Role or RDP**	**DCC Live Systems definition paragraph**
commissioningPartyFileSigning	The DCC	[Not Applicable]	(l)
requestingPartyFileSigning	The DCC	[Not Applicable]	(k)
s1SPMigrationSigning	The DCC	[Not Applicable]	(h)
commissioningPartyXmlSigning	The DCC	[Not Applicable]	(l)

Application of Section M (General)

3.17 The Responsible Supplier for each Device referred to in Clause 4.26 of this TMAD acknowledges that the carrying out of one or more of the steps referred to in this TMAD, at the request of the DCC, may result in the loss of Data stored on or in relation to each such Device and/or the ability to utilise the functionality of the Device. Neither the DCC nor the Installing Supplier shall be liable to the Responsible Supplier (or any other Party) for any Liability that arises from the carrying out of (or attempt to carry out) any of those steps, at the request of the DCC, where (and to the extent that) such person has acted in accordance with Good Industry Practice.

3.18 Where a Supplier Party has agreed with a SMETS1 SMSO that the SMETS1 SMSO shall not permit any third parties to communicate or otherwise interfere with a SMETS1 Installation (or any Devices forming part of it), then that Supplier Party confirms that that SMETS1 SMSO may permit the DCC to take the steps provided for in this TMAD which results in a communication or interference with that SMETS1 Installation (or any Devices forming part of it). Notwithstanding Section M11.6 of the Code, the SMETS1 SMSO shall be entitled to rely on and enforce the confirmation in this Clause 3.18 under the Contract (Rights of Third Parties) Act 1999.

3.19 It is acknowledged that each SMETS1 SMSO is acting as a DCC Service Provider when performing tasks ascribed to a SMETS1 SMSO under this TMAD (including where the SMETS1 SMSO provides services to the DCC in order for the DCC to carry out the tasks ascribed to a Requesting Party), and notwithstanding Section M11.6 of the Code, is therefore a person under Section M11.5 of the Code and entitled to rely on the waiver in Section M2.13(a) of the Code.

3.20 The DCC shall provide the Services described in this TMAD in accordance with Good Industry Practice. Each Installing Supplier shall act in accordance with Good Industry Practice when providing the support or assistance referred to in Clause 4.33.

3.21 The DCC shall take reasonable steps to ensure that any Data that is provided to it by each SMETS1 SMSO, for the purposes of Migration, is accurate.

3.22 Each Party’s liability under and in connection with this TMAD is limited in accordance with Section M2 (Limitations of Liability), provided that the liability of each of the DCC and each Installing Supplier for failing to act in accordance with Good Industry Practice in relation to the carrying out of (or attempt to carry out) one or more of the steps referred to in Clause 4.26

of this TMAD (and/or, in the case of the Installing Supplier, the provision of support or assistance referred to in Clause 4.33) shall be limited to £1,000,000 in the aggregate for each period of 12 months from the date this TMAD comes into effect (and from each anniversary of such date); and further provided that the DCC and/or relevant Installing Supplier will not be liable for a claim unless the claiming Party has given notice of such claim within six months of the occurrence of the relevant failure.

3.23 Where necessary, the provisions of Section M2.5(d) shall apply in relation to any liability that has been limited by the provisions of Clause 3.22.

<u>MPRN Validation for Leading Zeros</u>

3.24 In relation to SMETS1 Installations where GroupID = "AA", "BA", or "CA", each Supplier Party agrees that the DCC may ignore any leading zeros provided within the MPRN for a SMETS1 GSMS for the purposes of any validation steps under this TMAD.

<u>Provision of the current value of PINs</u>

3.25 Where GroupID = "CA", the DCC shall undertake the activities prescribed in this Clause 3.25 no later than 30 Working Days following this Clause 3.25 coming into effect. Where the PIN required to access functionality of the Gas Smart Metering System not meant for use by Energy Consumers (described in Clause 13.1 of the SMETS1 Supporting Requirements) was amended by the SMETS1 SMSO prior to this Clause 3.25 coming into effect:

(a) the DCC shall provide the current value of the PIN for the Gas Smart Metering System to the Installing Supplier for that Gas Smart Metering System and shall do so in an appropriately secure manner; and

(b) the Responsible Supplier consents to the provision of the PIN for the Gas Smart Metering System by the DCC to the Installing Supplier provided that such provision is done so in an appropriately secure manner.

4 <u>Pre-Migration Rights and Obligations</u>

4.1 Each Supplier Party shall provide any information that the DCC reasonably requests in order to support the planning, coordination and undertaking of (and ongoing support for) the Migration of SMETS1 Installations and shall do so in the timescales that the DCC reasonably requests.

4.1 A Where a Supplier Party is:

(a) not a DCC User; and

(b) the Responsible Supplier for one or more Dormant Meters and any associated devices;
the DCC may take reasonable steps to migrate SMETS1 Installations containing one or more such Dormant Meters without providing the various notifications and reports prescribed in this TMAD to the relevant Supplier Party that is not a DCC User.

4.1B Where a person:

(a) has ceased to be a Party; and

(b) is currently identified in the Registration Data as the Responsible Supplier for one or more Dormant Meters and any associated devices;

the DCC may take reasonable steps to migrate SMETS1 Installations containing one or more such Dormant Meters without providing the various notifications and reports prescribed in this TMAD for a Responsible Supplier.

4.1C Where,

(a) the SMETS1 Installation contains solely Dormant Meter(s); and

(b) either the MPAN, MPRN, or both for the SMETS1 Installation are recorded either:

(i) in multiple SMETS1 SMSOs; or

(ii) in at least one SMETS1 SMSO and the Smart Metering Inventory against SMETS2+ Devices;

the DCC may take reasonable steps to verify that the SMETS1 Installation with the latest installation date is the only SMETS1 Installation communicating with a SMETS1 SMSO and no SMETS2+ Devices are communicating with DCC Systems in order to allow Migration of the SMETS1 Installation to subsequently commence based on a deemed authorisation pursuant to Clause 4.27.

4.2 Where, and to the extent notified by the DCC, each Supplier Party may request that the DCC undertakes early validation of any Migration Common Files pertaining to SMETS1 Installations comprising an Active Meter for which it is the Responsible Supplier. To enable this, the DCC shall permit each SMETS1 SMSO to make arrangements with the relevant

Requesting Party to enable the submission of Migration Common Files for early validation purposes, provided that such files shall be submitted to a different location from those submitted by the Requesting Party pursuant to Clause 5.8. When the DCC receives such a file, it shall carry out the steps required by Clauses 5.9 and 5.10.

4.3 Subject to Clause 4.24, the DCC shall, on any day during which it is carrying out the Migration of SMETS1 Installations, take reasonable steps to Migrate relevant SMETS1 Installations flagged as a priority prior to SMETS1 Installations not flagged as a priority.

4.4 Where, by virtue of this TMAD, the DCC is required to consult on the content of any document with the Panel, all Parties, the Authority and (on request) the Secretary of State prior to such a document taking effect, this requirement may be satisfied by the undertaking of consultation on such content prior to this TMAD coming into effect.

Indicative Migration Forecasts and Migration Demand Commitment

4.5 For the purposes of supporting the planning and coordination of the Migration of SMETS1 Installations, by no later than the 20th day of each month, each Responsible Supplier shall provide an Indicative Migration Forecast to the DCC for each SMETS1 SMSO. Such forecast shall, at a minimum, be broken down by Electricity Distributor and shall be provided in relation to any SMETS1 SMSOs in relation to which Migration is due to commence within the next six months (as set out in the SMETS1 Services delivery plan produced pursuant to condition 13 of the DCC Licence).

4.6 By the end of each month, the DCC shall provide all Parties, the Panel, the Authority and the Secretary of State with a summary report that aggregates information from all Indicative Migration Forecasts showing the aggregate forecast number of SMETS1 Installation Migrations per day and per SMETS1 SMSO.

4.7 The DCC may provide to a SMETS1 SMSO all Indicative Migration Forecasts provided to it by Responsible Suppliers that pertain to that SMETS1 SMSO.

4.8 The DCC and each Responsible Supplier shall schedule the Migration of SMETS1 Installations comprising an Active Meter(s) that pertain to a particular SMETS1 SMSO in each Migration Week in accordance with the following process:

(a) by no later than 15.00 hours on the Monday that falls two weeks prior to each Migration Week, each Responsible Supplier shall notify the DCC, of the number of SMETS1 Installations in relation to which it reasonably expects to submit Migration Authorisations for each day of that

Migration Week, per day and identify the number of those SMETS1 Installations per day per SMETS1 SMSO (the "Daily Migration Demand") and this Daily Migration Demand will be dis-aggregated by Electricity Distributor;

(b) by no later than 10.00 hours on the Tuesday that falls two weeks prior to each Migration Week, the DCC shall confirm to each Responsible Supplier the number of SMETS1 Installations that the DCC is committing to Migrate on each day within that Migration Week for that Responsible Supplier per SMETS1 SMSO (the "Migration Demand Commitment"), which shall, subject to Clause 4.11, be the same as the Responsible Supplier's Daily Migration Demand; and

(c) by no later than 17.00 hours on that same following Tuesday, the DCC shall provide all Parties, the Panel, the Authority and the Secretary of State with a summary report that aggregates information from all Migration Demand Commitments, which includes the number of SMETS1 Installations dis-aggregated by Electricity Distributor in that Migration Week per SMETS1 SMSO, or where necessary a pro-rata estimate of this.

4.9 Where a Responsible Supplier does not notify the DCC of the Responsible Supplier's Daily Migration Demand for any particular Migration Week in accordance with Clause 4.8(a), the DCC shall use zero for the values of Daily Migration Demand for that Responsible Supplier for the purposes of its migration scheduling in relation to that Migration Week.

4.10 Where pursuant to Clause 4.8(b), the DCC fails to confirm the Migration Demand Commitment for a Responsible Supplier, the DCC shall be deemed to have agreed to and confirmed that the Responsible Supplier's Daily Migration Demand for each day per SMETS1 SMSO within the relevant Migration Week is that Supplier's Daily Migration Demand Commitment.

4.11 Where the DCC reasonably considers that it cannot commit to the value for a Daily Migration Demand for one or more days within any future Migration Week, the DCC shall set each Responsible Supplier's Daily Migration Demand Commitment in accordance with the rules set out in a document for that purpose (the "**Migration Scaling Methodology**"), as described in Clause 4.12.

4.12 The DCC shall make available to the Panel, all Parties, the Authority and (on request) the Secretary of State the Migration Scaling Methodology, as follows:

(a) the DCC shall

(i) establish and periodically review the Migration Scaling Methodology, and shall consult with the Panel, the Parties and the Authority on the content of or any subsequent modification to the Migration Scaling Methodology prior to it taking effect; and

(ii) may modify the Migration Scaling Methodology without consultation where the modification is of a minor typographical nature or where the modification has no material effect on the rights or obligations of Parties; and

(b) at least 14 days prior to the coming into effect of the Migration Scaling Methodology or any subsequent revision to it, the DCC shall provide a copy of that document to the Panel, the Parties, the Authority and the Secretary of State, and publish a copy of it on the DCC Website.

4.13 Except in the case of modification to the Migration Scaling Methodology made pursuant to Clause 4.12 (a) (ii), where a Party disagrees with the content of any version of the Migration Scaling Methodology, the Party may (within one month of that version coming into effect) refer the matter to the Secretary of State for their determination, which determination shall be final and binding for the purposes of the Code. In the event that such referral is made the new version of the Migration Scaling Methodology published by the DCC shall apply prior to any such determination.

4.14 The DCC shall, in relation to each Responsible Supplier, take all reasonable steps to Migrate each day a number of SMETS1 Installations that contain one or more Active Meters for which that Supplier Party is the Responsible Supplier that is equal to the number within the Migration Demand Commitment for that Responsible Supplier, subject to having received the necessary Migration Authorisation to do so. For each Migration Week, the DCC shall, as soon as reasonably practicable, notify the relevant Responsible Supplier where the DCC reasonably considers that it will only be able to Migrate a number of SMETS1 Installations for that Responsible Supplier that is materially less than the number within the Migration Demand Commitment for that Responsible Supplier.

4.15 For each Responsible Supplier, the DCC may Migrate further SMETS1 Installations each day in excess of the Migration Demand Commitment for that Responsible Supplier where the DCC considers it is reasonable to undertake such additional Migrations and where a Migration Authorisation has been submitted for the excess. It is acknowledged that, in the case of Group ID = “EA” or “EB”, the Migration might not complete within the day.

Pre-conditions for Migration

4.16 The Requesting Party shall not commence the Migration of any SMETS1 Installation that does not correspond to an entry on the SMETS1 Eligible Product Combinations.

4.17 The Requesting Party shall not commence the Migration of any SMETS1 Installation until the DCC has received (or is deemed to have received in accordance with Clause 4.27 or the definition of Migration Authorisation) a Migration Authorisation from the Responsible Supplier or Responsible Suppliers for that SMETS1 Installation.

4.18 Each Supplier Party agrees that where the DCC has received (or is deemed to have received in accordance with Clause 4.27 or the definition of Migration Authorisation) such Migration Authorisation(s), it may carry out the steps to Migrate that SMETS1 Installation in accordance with the provisions of this TMAD.

4.19 Where there is more than one Responsible Supplier for a SMETS1 Installation and where the DCC has received Migration Authorisations from both such Responsible Suppliers which authorise the Migration of that SMETS1 Installation on different days in the same Migration Week, the Requesting Party shall take steps to initiate the Migration of that SMETS1 Installation in timescales consistent with the later of those two days. In such circumstances, the Migration Authorisation provided by the Responsible Supplier for the earlier of the two days is deemed amended to constitute a Migration Authorisation for the later of those two days.

4.20 Each Supplier Party agrees that each SMETS1 SMSO and the DCC may exchange any information (including Secret Key Material) that is reasonably needed for the DCC to discharge any of its obligations under this TMAD.

4.21 The DCC shall, from time to time, use and rely upon (and shall, subject to Clause 3.21, have no liability arising from any inaccuracy in) the information provided to it by each SMETS1 SMSO for the purposes of this TMAD, including:

(a) the Device IDs of Devices that are to be Migrated;

(b) the status of Devices, being ‘Dormant Meter’, ‘Active Meter’ or ‘Active GPF’;

(c) MPANs and MPRNs associated with Devices; and

(d) the content of Migration Common Files, Migration Group Files and Migration Group Encrypted Files.

4.22 This TMAD constitutes each Responsible Supplier’s documented instructions to the DCC and each SMETS1 SMSO to Process any Personal Data required for the purposes of Migration of SMETS1 Installations.

4.23 With the exception of GroupID = “DA”, the DCC shall, where requested to do so by a

Responsible Supplier for one or more SMETS1 Installations comprising an Active Meter for which that Supplier is the Responsible Supplier, take all reasonable steps not to start the Migration of those SMETS1 Installations notwithstanding that the DCC has previously received a Migration Authorisation in respect of them from the Responsible Supplier.

4.23A For GroupID = “DA” where requested by a Responsible Supplier, the DCC shall take all reasonable steps not to start the Migration of any SMETS1 Installation for which that Supplier Party is a Responsible Supplier for one (or both) Active Meters. The effect of this shall be that where DCC can accommodate the request, the DCC shall not start the Migration of any of the SMETS1 Installations contained in any Migration Authorisation received from that Responsible Supplier that are due to commence on the same day as the SMETS1 Installation(s) that was the subject of the request, for which the Migration has not yet commenced.

Dormant Meters

4.24 The DCC shall take all reasonable steps to Migrate SMETS1 Installations comprising only Dormant Meters, including arranging for any pre-requisite steps set out in this TMAD to be undertaken. The DCC shall Migrate such SMETS1 Installations comprising only Dormant Meters as soon as reasonably practicable, which shall include giving priority to the Migration of SMETS1 Installations comprising only Dormant Meters over and above SMETS1 Installations which include one or more Active Meters.

4.25 Each Responsible Supplier for each SMETS1 CHF that forms part of a SMETS1 Installation that includes one or more Dormant Meters agrees that the relevant SMETS1 SMSO may, where requested to do so by the DCC, initiate remote communications with that SMETS1 CHF in order to confirm whether or not the SMETS1 SMSO is capable of remotely communicating with that SMETS1 CHF.

4.26 The Responsible Supplier for each Dormant Meter and any associated Devices for which it is also the Responsible Supplier that form part of a SMETS1 Installation agrees that the relevant SMETS1 SMSO may, where requested to do so by the DCC, take any steps reasonably necessary in order to ensure that the Devices are configured in accordance with the requirements of the SMETS1 Supporting Requirements and Clause 5.12(e) of this TMAD, and/or such that the Devices form part of a SMETS1 Installation that comprises an entry on the list of Eligible Product Combinations, including upgrading the firmware on the Devices for those purposes. The Responsible Supplier for each Dormant Meter and any associated Devices for which it is also the Responsible Supplier that form part of a SMETS1 Installation agrees that the relevant SMETS1 SMSO may, where requested to do so by the DCC, take any steps reasonably necessary in order to upgrade the firmware on the Devices such that the Devices form part of an entry that is planned to be listed on the Eligible Product Combinations. For the purposes of this Clause 4.26, an entry is planned to be listed on the Eligible Product Combinations where pursuant to the SEC Variation Testing Approach Document for SMETS1 Services:

(a) a Completion Report for the Migration Test Phase and SIT Test Phase regarding the planned entry on the list of Eligible Product Combinations has been approved by the Testing Advisory Group of the Panel ("TAG"); or

(b) a DMCT EPCL Report has been issued in respect of the planned entry on the list of Eligible Product Combinations.

4.26A The DCC shall instruct the SMETS1 SMSO to de-register the Gas Meter from the SMETS1 Installation within their SMETS1 SMSO system where:

(a) [NOT USED];

(b) such SMETS1 Installation contains solely Dormant Meters;

(c) the firmware has successfully upgraded and configuration applied for the Electricity Meter within such SMETS1 Installation such that the Devices, excluding the Gas Meter, form part of a SMETS1 Installation that comprises an entry on the list of Eligible Product Combinations;

(d) the firmware has not successfully upgraded and/or configuration not applied for the Gas Meter within such SMETS1 Installation (having taken all reasonable steps pursuant to Clause 4.26); and

(e) the DCC reasonably believes that:

(i) there is not another entry to the list of SMETS1 Eligible Product Combinations that it could propose which, were it to be approved by the Secretary of State, would enable the Migration of that SMETS1 Installation to be attempted without firmware upgrade for the Gas Meter; and

(ii) such SMETS1 Installation would be capable of successful Migration were an appropriate entry added to the list of SMETS1 Eligible Product Combinations.

4.26B The DCC shall instruct the SMETS1 SMSO to de-register the Gas Meter from the SMETS1 Installation within their SMETS1 SMSO system where:

(a) GroupID = “CB” or “DA”;

(b) such SMETS1 Installation contains solely Dormant Meters;

(c) the GT01 check has failed at least three times;

(d) each such failure is in a separate and non-contiguous Migration Week; and

(e) each such failure is at either:

(i) GT01, sub-step 4 in Table A3 where GroupID = “CB”; or

(ii) GT01, sub-step 2 in Table C2 where GroupID = “DA”,

4.26C The Responsible Supplier for each Gas Meter referred to in either Clause 4.26A or Clause 4.26B, authorises the DCC to instruct the SMETS1 SMSO take the steps to deregister the Gas Meter within the relevant SMETS1 Installation.

4.26D The DCC may instruct the SMETS1 SMSO to de-register the SMETS1 PPMID from the SMETS1 Installation within their SMETS1 SMSO system where:

(a) Group ID = “EA”;

(b) such SMETS1 Installation contains solely Dormant Meters;

(c) due to invalid data for the SMETS1 PPMID, the DCC has been unable to propose an entry on the list of SMETS1 Eligible Product Combinations that would allow the Migration of the SMETS1 Installation to commence; and

(d) the Devices, excluding the SMETS1 PPMID, form part of a SMETS1 Installation that comprises an entry on the list of SMETS1 Eligible Product Combinations.

4.26E Both the Responsible Supplier for the ESME and the Responsible Supplier for the GSME (where present) within the SMETS1 Installation referred to in Clause 4.26D, authorises the DCC to instruct the SMETS1 SMSO to take the steps to deregister the SMETS1 PPMID within the relevant SMETS1 Installation.

4.27 The Responsible Supplier for each Device referred to in Clause 4.26, authorises the DCC to take the steps and carry out the processing set out in this TMAD in order to Migrate the relevant SMETS1 Installation (and is therefore deemed to have given a Migration Authorisation in respect of that SMETS1 Installation).

4.28 Where a SMETS1 Installation includes both an Active Meter and a Dormant Meter, the DCC shall not commence the Migration unless it has received a Migration Authorisation from the Responsible Supplier for the Active Meter in relation to that SMETS1 Installation.

4.29 Where the DCC plans to carry out the steps referred to in Clause 4.26 in relation to any SMETS1 Installation which includes Dormant Meters (but no Active Meters), the DCC shall notify the Responsible Supplier(s) for that SMETS1 Installation at least 5 Working Days (or 2 Working Days in the case of Recently Dormant SMETS1 Installations) (or fewer where mutually agreed between the DCC and the Responsible Supplier(s) for that SMETS1 Installation) before the earliest scheduled date for undertaking those steps. Where there are two Responsible Suppliers for the Smart Metering Systems that together comprise the same SMETS1 Installation that contains only Dormant Meters, and they are Affiliates of one another, then the DCC may issue such notification only to the Responsible Supplier for the Electricity Smart Metering System and the Responsible Supplier for the Gas Smart Metering System shall be deemed to have received a notification for the purpose of this Clause 4.29. Where there is a change of Responsible Supplier after the DCC has issued such notification, the DCC may continue to carry out the relevant steps as planned and shall take reasonable steps to notify the new Responsible Supplier prior to carrying them out.

4.30 Where the DCC plans to carry out the steps referred to in Clause 4.27 in relation to any SMETS1 Installation which includes Dormant Meters (but no Active Meters), the DCC shall notify the Responsible Supplier(s) for that SMETS1 Installation at least 15 Working Days (or 8 Working Days in the case of Recently Dormant SMETS1 Installations) (or fewer where mutually agreed between the DCC and the Responsible Supplier(s) for that SMETS1 Installation) before the earliest scheduled date for undertaking those steps. Where there are two Responsible Suppliers for the Smart Metering Systems that together comprise the same SMETS1 Installation that contains only Dormant Meters, and they are Affiliates of one another, then the DCC may issue such notification only to the Responsible Supplier for the Electricity Smart Metering System and the Responsible Supplier for the Gas Smart Metering System shall be deemed to have received a notification for the purpose of this Clause 4.30. Where there is a change of Responsible Supplier after the DCC has issued such a notification, the DCC may continue to carry out the relevant steps as planned and shall take reasonable steps to notify the new Responsible Supplier prior to carrying them out.

4.31 Notifications sent by the DCC pursuant to Clause 4.29 or Clause 4.30 shall be processed in accordance with the Migration Authorisation Mechanism and shall include, as a minimum, in relation to each SMETS1 Installation:

(a) the date from which the DCC has scheduled the relevant activities;

(b) the relevant MPANs and MPRNs;

(c) the Device ID for each relevant Device;

(d) the device serial number (according to information held by the relevant SMETS1 SMSO) for each relevant Device; and

(e) where such notification is sent pursuant to Clause 4.29, the Device Model Combination that the DCC intends should result from any firmware upgrades that it plans to instruct in relation to the relevant Device(s).

4.32 Where a Responsible Supplier receives a notification from DCC pursuant to Clause 4.30 the Responsible Supplier may respond in the manner set out in the Migration Authorisation Mechanism to flag any notified SMETS1 Installation as a priority and/ or to specify the Supplier and/or Network Operator Certificate IDs that it wishes the DCC to include in Commissioning Requests that it processes in relation to any notified SMETS1 Installation. Where there are two Responsible Suppliers for the Smart Metering Systems that together comprise the same SMETS1 Installation, and they are Affiliates of one another, then the Responsible Supplier for the Electricity Smart Metering System may specify the Supplier and/or Network Operator Certificate IDs that it wishes the DCC to include in Commissioning Requests in respect of the Gas Smart Metering System, in which case the Responsible Supplier for the Gas Smart Metering System shall be deemed to have specified those Supplier and/or Network Operator Certificate IDs. The DCC shall only be obliged to consider such information where it is received within the timescales set out in the Migration Authorisation Mechanism but may use such information submitted after these timescales if it is practicable to do so. A Supplier Party may only request that a SMETS1 Installation is treated as a priority for Migration purposes where the type of Energy Consumer at the premises for that SMETS1 Installation requires it to be prioritised over and above the Migration of other SMETS1 Installations.

4.32A For the purposes of Migration, the DCC shall disregard any Network Operator Certificate IDs for a Gas Transporter provided by the Responsible Supplier (pursuant to Clause 4.32) where that Network Operator Certificate ID has previously resulted in at least five Migration failures for the SMETS1 Installation due to a failure of the check at either 5.10.16 or 5.10.17 as set out in Table 5.10.

4.33 Any Supplier Party that is an Installing Supplier for any of the Dormant Meters and associated Devices referred to in Clause 4.26 shall take all reasonable steps to provide such support and assistance as the DCC may reasonably request (including where they exist, the provision of firmware for each such Device) in order that the DCC or the relevant SMETS1 SMSO is capable of carrying out the steps set out in Clause 4.26. For the purposes of carrying out the steps that are set out in Clause 4.26, the DCC and/or any relevant SMETS1 SMSO shall rely on (and shall have no liability arising from any inaccuracy in) the firmware that is provided to the DCC by an Installing Supplier together with the relevant information that supports the sequencing of the required firmware upgrades, unless it is (or should reasonably have been) apparent to the DCC that the firmware or relevant information that has been provided to the DCC is not suitable.

4.34 The DCC shall provide to any Supplier Party upon request relevant excerpts from the information provided to it pursuant to Clause 4.33 in relation to sequencing of firmware upgrades and/or configuration of devices. No Party shall have any liability arising from any inaccuracy in the information provided by the DCC pursuant to this Clause 4.34.

4.34A Where there is more than one SMETS1 PPMID, SMETS1 IHD or SMETS1 CAD in a SMETS1 Installation, that is comprised solely of Dormant meters, the DCC shall include only one of each Device Type in the Migration Common File, which shall be the one that was most recently joined to the HAN. Any SMETS1 PPMID, SMETS1 IHD or SMETS1 CAD for which there is insufficient information in order to populate the Migration Common File shall not be included in the MCF and therefore shall not be Migrated.

Migration Authorisations and the Migration Authorisation Mechanisms

4.35 The DCC shall set out and make available to all Supplier Parties the proposed mechanism (the "Migration Authorisation Mechanism") which shall, in addition to the matters set out in Clauses 4.29 to 4.32, provide the means by which:

(a) a Migration Authorisation may be provided by the Responsible Supplier(s) for a SMETS1 Installation comprising one or more Active Meters to the Requesting Party;

(b) where the Responsible Supplier is the Responsible Supplier for all Devices comprising a SMETS1 Installation comprising only Active Meters, the Responsible Supplier shall indicate whether it wishes the Commissioning Party to carry out the steps necessary to Commission the Devices comprising that SMETS1 Installation or, alternatively that the Responsible Supplier wishes itself to carry out these steps, being, as further described in Clauses 4.37 to 4.40; and

(c) Clause 4.35 (b) shall also apply where there are two Responsible Suppliers for the Smart Metering Systems that together comprise the same SMETS1 Installation comprising only Active Meters, and they are Affiliates of one another, in which case the Responsible Supplier for the Electricity Smart Metering System shall give the required indication on behalf of itself and the Responsible Supplier for the Gas Smart Metering System (and any such indication shall be deemed to constitute an indication by the Responsible Supplier for the Gas Smart Metering System) provided that the indication is either that both Responsible Suppliers wish the Commissioning Party to carry out the steps, or both Responsible Suppliers wish themselves to carry out the steps.

4.36 Where a SMETS1 Installation includes any Dormant Meter, the steps that are necessary to Commission the Devices that comprise that SMETS1 Installation shall only be carried out by the Commissioning Party.

4.37 Where a SMETS1 Installation includes both an Active Meter and a Dormant Meter, the DCC shall notify the Responsible Supplier, that is the Responsible Supplier for the Active Meter in relation to that SMETS1 Installation, by no later than 23:59 on the Thursday that falls three days prior to the Migration Week in which that SMETS1 Installation is scheduled to commence Migration, that the SMETS1 Installation includes a Dormant Meter. Where the DCC receives a Migration Authorisation after the timescales for receipt set out in the Migration Authorisation Mechanism the DCC may still process Migrations based on the Migration Authorisation but shall not be obliged to do so.

4.38 The Migration Authorisation Mechanism shall require that the Responsible Supplier(s) for a SMETS1 Installation for which a Migration Authorisation is being provided shall provide the MPRN for each SMETS1 GSMS and/or the MPAN for each SMETS1 ESMS that forms part of that SMETS1 Installation. The Migration Authorisation Mechanism shall require that, in relation to each SMETS1 Device that forms part of a SMETS1 Installation for which Migration Authorisation is being provided, the Responsible Supplier for each Device listed in Table 4.38 shall provide the information required in that table for that Device. Where there are two Responsible Suppliers for the Smart Metering Systems that together comprise the same SMETS1 Installation comprising only Active Meters, and they are Affiliates of one another, the Responsible Supplier for the Electricity Smart Metering System may provide the required information for the SMETS1 ESME on behalf of itself and the required information for the SMETS1 GPF and SMETS GSME on behalf of the Responsible Supplier for the Gas Smart Metering System and this shall be deemed to constitute provision by the Responsible Supplier for the Gas Smart Metering System.

Device	**Required information**
SMETS1 ESME	CriticalSupplierCertificateID NonCriticalSupplierCertificateID
SMETS1 GPF	CriticalSupplierCertificateID NonCriticalSupplierCertificateID
SMETS1 GSME	CriticalSupplierCertificateID NonCriticalSupplierCertificateID

Table 4.38

4.39 The Migration Authorisation Mechanism shall require the Responsible Supplier that submits the Migration Authorisation to Digitally Sign communications containing Migration Authorisations using a Private Key associated with an IKI Certificate that has been Issued to an Authorised Responsible Officer of that Responsible Supplier. More generally the DCC and Supplier Parties may use Private Keys associated with IKI Certificates that have been Issued to their Authorised Responsible Officers in order to Digitally Sign communications in relation to the Migration Authorisation Mechanism.

4.40 The Migration Authorisation Mechanism shall allow the Responsible Supplier to flag any SMETS1 Installation as a priority and/or to specify the Network Operator Certificate IDs that it wishes the DCC to include in Commissioning Requests that it processes. Where there are two Responsible Suppliers for the Smart Metering Systems that together comprise the same SMETS1 Installation, and they are Affiliated of one another, then the Responsible Supplier for the Electricity Smart Metering System may provide the Network Operator Certificate ID in respect of the Gas Smart Metering System, in which case the Responsible Supplier for the Gas Smart Metering System shall be deemed to have specified that Network Operator Certificate ID. A Supplier Party may only request that a SMETS1 Installation is treated as a priority for Migration purposes where the type of Energy Consumer at the premises for that SMETS1 Installation requires it to be treated as a priority.

4.41 The DCC shall, following consultation with Supplier Parties and after taking into account any comments that have been provided to it, publish the Migration Authorisation Mechanism to all Supplier Parties, together with the date on which it intends that the Migration Authorisation Mechanism shall come into effect, which shall be not less than 14 days from the date of publication.

4.42 Following DCC's publication of the Migration Authorisation Mechanism and in accordance with the requirements of Clause 4.41 and prior to DCC's published date for the coming into effect of the Migration Authorisation Mechanism, any Supplier Party that wishes to object to the Migration Authorisation Mechanism may refer the matter to the Secretary of State for a determination, which determination shall be final and binding for the purposes of this TMAD.

4.43 The DCC may, from time to time, update the Migration Authorisation Mechanism, provided that the DCC shall ensure that the most up to date Migration Authorisation Mechanism is published to all Supplier Parties at all times. The processes set out in Clauses 4.41 and 4.42 shall apply to any modification of the Migration Authorisation Mechanism, except where the modification is of a minor typographical nature or where the modification has no material effect on the rights or obligations of Parties. Where the modification is of a minor typographical nature or where the modification has no material effect on the rights or obligations of Parties, the DCC shall publish the updated Migration Authorisation Mechanism to all Supplier Parties, together with the date on which it intends that the updated Migration Authorisation Mechanism shall come into effect, which shall be not less than 14 days from the date of publication. The Migration Authorisation Mechanism published by the DCC shall have effect unless or until the Secretary of State determines otherwise.

4.44 The Responsible Supplier for each Active Meter and any associated Devices for which it is also the Responsible Supplier that form part of a SMETS1 Installation shall ensure that, prior to its Migration, the Devices that form part of that SMETS1 Installation are configured in accordance with the requirements of SMETS1 Supporting Requirements of this TMAD, and/or the Devices form part of a SMETS1 Installation that comprises a Device Model Combination that is listed on the Eligible Product Combinations, including upgrading the firmware on the Devices for those purposes.

4.44A Where there is more than one SMETS1 PPMID, SMETS1 IHD or SMETS1 CAD in a SMETS1 Installation, that is comprised of Active or Mixed Installations, the DCC shall include only one of each Device Type in the Migration Common File, which shall be the one that was most recently joined to the HAN. Any SMETS1 PPMID, SMETS1 IHD or SMETS1 CAD for which there is insufficient information in order to populate the Migration Common File shall not be included in the MCF and therefore shall not be Migrated.

Migration Reporting

4.45 The DCC shall make available to the Panel, all Parties and (on request) the Secretary of State the “Migration Reporting Regime” that list the reports that the DCC shall provide on Migration and provides an overview of the frequency, content of and recipients of those reports, as follows:

(a) the DCC:

(i) shall establish and periodically review the Migration Reporting Regime, and shall consult with the Panel, the Parties and the Authority on the content of or any subsequent modification to the Migration Reporting Regime prior to it taking effect; and

(ii) may modify the Migration Reporting Regime without consultation where the modification is of a minor typographical nature or where the modification has no material effect on the rights or obligations of Parties; and

(b) at least 14 days prior to the coming into effect of the Migration Reporting Regime or any subsequent revision to it, the DCC shall provide a copy of that document to the Panel, the Parties, the Authority and the Secretary of State, and publish a copy of it on the DCC Website.

4.46 Where a Party considers that the reporting provided for in the Migration Reporting Regime made pursuant to Clause 4.45 is insufficient, the Party may (within one month of the document being provided under Clause 4.45) refer the matter to the Secretary of State for determination, which determination shall be final and binding for the purposes of this TMAD. In the event that such referral is made the new version of the Migration Reporting Methodology published by the DCC shall apply prior to any such determination.

Electricity Distributor Network Operator Certificate IDs

4.47 The DCC shall establish a reasonable process by which Electricity Distributors can notify the DCC of the Network Operator Certificate IDs that they wish the DCC to include in Commissioning Requests that the DCC processes in relation to SMETS1 ESMEs and shall inform Electricity Distributors of that notification process. The process shall allow an Electricity Distributor to change from time to time the Network Operator Certificate IDs that have been notified.

4.48 Where in relation to a SMETS1 ESME, the Responsible Supplier has not specified to the DCC either or both of the Electricity Distributor’s Network Operator Certificate IDs in accordance with the Migration Authorisation Mechanism (for a SMETS1 ESME that is either an Active Meter or a Dormant Meter except where the SMETS1 ESME is a Dormant Meter and there is a SMETS1 GSME that is an Active Meter within the same SMETS1 Installation), the DCC shall (unless the DCC has identified that the relevant MPAN is invalid) ensure that, for any such unspecified Network Operator Certificate IDs, the latest Network Operator Certificate IDs that have been notified by the Electricity Distributor under Clause 4.47 are included in relation to the relevant Devices within any Migration Common File sent by the relevant Requesting Party.

Change of Supplier Events

4.49 The Responsible Supplier for any Meter:

(a) that forms part of an Enrolled Smart Metering System;

(b) that forms part of a SMETS1 Installation where GroupID = "EA";

(c) that was operating in Prepayment Mode (with its SMETS1 meaning) at the time that the SMETS1 Installation of which it formed part was Migrated;

(d) which has continued to operate in Prepayment Mode (with its SMETS1 meaning) since that time;

(e) in relation to which a "Top Up" Service Request has not been successfully processed since the Meter was Commissioned;

(f) that has not been the subject of a change of supplier event since the Meter was Commissioned; and

(g) in relation to which a change of supplier event is pending,

shall ensure that the Payment Mode (with its SMETS1 meaning) of the Meter is set to Credit Mode (with its SMETS1 meaning) by the time that the change of supplier event occurs.

5 Migration Process

Setup steps

5.1 Before the DCC adds an entry to the SMETS1 Eligible Product Combinations, the DCC shall, for the Group which includes Devices with the corresponding combination of Device Models:

(a) notify to the relevant SMETS1 SMSO any Public Keys that are to be used to create any required EncryptedS1SPGroupInformation or MasterKeyInformation elements and for each such Public Key:

(i) the Key Identifier (see X509SKI);

(ii) the inclusive start and end dates of the period during which the Public Key may be used; and

(iii) any constraints as to the part(s) of the Group in relation to which the Public Key can be used;

(b) notify to the relevant SMETS1 SMSO either:

(i) the technical details and associated steps that would be required in order to configure Devices within such SMETS1 Installations and any associated systems, including those required by ‘Pre-enrolment Configuration Requirements’ for the specified GroupID, so as to be able to communicate with the DCC Live Systems; or

(ii) a statement that no such configuration would be required for Devices comprising such SMETS1 Installations; and

(c) where GroupID = “EA” or “EB”, receive from the relevant SMETS1 SMSO any certificates required to restore communication to the SMETS1 SMSO in the event of a rollback along with:

(i) the inclusive start and end dates of the period during which the certificates may be used; and

(ii) any constraints as to the use of the certificates.

5.2 When the DCC adds an entry to the SMETS1 Eligible Products Combinations, the DCC shall include within it the associated GroupID with that entry.

5.3 Any Private Key, which is associated with a Public Key published pursuant to Clause 5.1 for use in creating MasterKeyInformation elements, shall be generated by, and known only to, the relevant DCO.

5.4 Any Private Key, which is associated with a Public Key published pursuant to Clause 5.1 for use in creating EncryptedS1SPGroupInformation elements, shall be generated by, and known only to, the relevant S1SP.

5.4A Before the DCC adds the first entry to the SMETS1 Eligible Product Combinations with a GroupID = “DA”, the DCO shall generate at least one Private Key and corresponding Public Key(s) for that GroupID to be used solely in relation to ‘Securing a SMETS1 GSME’ and ‘Securing a SMETS1 ESME’ for that GroupID in Appendix C. Such Private Key(s) shall be generated by, and known only to, the relevant DCO.

<u>Digital Signature</u>

5.5 In relation to the Digital Signing obligations in this TMAD, Parties shall only accept as valid Digital Signatures which authenticate against Certificates with Remote Party Roles conforming to Table 5.5. The Parties identified in Table 5.5 shall only sign using Private Keys where the corresponding Public Keys have been incorporated in Organisation Certificates with the corresponding Remote Party Role.

Object to which signature relates	**Party Digitally Signing**	**Required Remote Party Role in the Certificate used to check signature**
Commissioning Outcome File	Commissioning Party	commissioningPartyFileSigning
Migration Common File	Requesting Party	requestingPartyFileSigning
Migration Group File	Requesting Party	requestingPartyFileSigning
Migration Group Encrypted File	Requesting Party	requestingPartyFileSigning
Migration Common Validation File	S1SP	s1SPMigrationSigning
S1SP Commissioning File	S1SP	s1SPMigrationSigning
XML documents created to comply with the DUIS Schema	Commissioning Party	commissioningPartyXmlSigning

Table 5.5

Counters

5.6 Each Requesting Party, each S1SP and the Commissioning Party shall maintain counters, which are sequentially increased for each file created, according the requirements of Table 5.7 so that the files each creates shall, except in cases of replay, pass the anti-replay checks specified in Table 5.9.

5.7 Where an entity acts as the Authenticator with respect to the checks and processing required by Table 5.9, it shall have the capacity to establish and maintain the counters in the ‘Counter of Authenticator’ column of Table 5.7 in the way required by Table 5.9.

File Type	Party creating the file	Counter of file creator	Counter of Authenticator
Commissioning Outcome File	Commissioning Party	Commissioning Outcome File Counter	Commissioning Outcome File Stored Counter
Migration Common File	Requesting Party	Migration Common File Counter. For clarity, this counter shall be included, along with RequestingPartyID, in all files related to this Migration Common File. Other counters shall additionally be included in all such related files.	Migration Common File Stored Counter
Migration Group File	Requesting Party	Migration Group File Counter	Migration File Group Stored Counter
Migration Group Encrypted File	Requesting Party	Migration Group Encrypted File Counter	Migration File Group Encrypted Stored Counter
Migration Common Validation File	S1SP	Migration Common Validation File Counter	Migration File Common Validation Stored Counter
S1SP Commissioning File	S1SP	S1SP Commissioning File Counter	S1SP Commissioning File Stored Counter

Table 5.7

Creation and validation of standard information

5.8 Before the Migration of any set of SMETS1 Installations is triggered pursuant to Clause 5.12, the Requesting Party shall create, populate with details of that set of SMETS1 Installations, Digitally Sign and then submit to the DCC a Migration Common File adhering to 'Migration Common File Device Selection Requirements' for the specific GroupID, as specified in the Group Specific Requirements. Except where the GroupID is "EA" or "EB", the Requesting Party shall not include in any Migration Common File details for any Active Device where either the CriticalSupplierCertificateID or NonCriticalSupplierCertificateID have the null value. The Requesting Party may only set the ToBeCommissionedByDCC to be False where the Migration Common File only contains details on Active Devices.

The Requesting Party shall set ToBeCommissionedByDCC to ‘True’ unless:

(i) all of the Devices that form such a SMETS1 Installation are Active Devices; and

(ii) the Responsible Supplier (or a Responsible Supplier to which it is Affiliated) has indicated, pursuant to Clause 4.35(b), that it wishes to carry out the steps to commission all such Devices; and

(iii) all Supplier Certificate IDs within the file refer to Certificates all of which contain User IDs allocated to the same Supplier Party (or allocated to multiple Supplier Parties provided that they are all Affiliates of one another).

5.8A For Group ID = “EA” or “EB”, where a Migration in respect of a SMETS1 Installation cannot successfully complete and it is not possible to rollback that SMETS1 Installation to the SMETS1 SMSO, but, in the reasonable opinion of the DCC, the Migration ought to be capable of successfully completing were a new Migration Common File to be submitted in respect of that SMETS1 Installation, then the DCC shall instruct the Requesting Party to submit a new Migration Common File. For the avoidance of doubt, such submission does not constitute a commencement of the Migration in respect of that SMETS1 Installation.

5.8B For each SMETS1 Installation where the SMETS1 GSME is a Dormant Meter and:

(a) where GroupID = “AA”, “BA”, or “CA”;

(b) the GT01 check has failed at least three times (since 4 November 2021);

(c) each such failure is in a separate and non-contiguous Migration Week;

(d) each such failure is at GT01, sub-step 4 in Table A3; and

(e) the Payment Mode (with its SMETS1 meaning) of the Gas Meter is set to Credit Mode (with its SMETS1 meaning);

then the DCC shall exclude the SMETS1 GSME from the SMETS1 Installation in the generation of subsequent Migration Common File(s), notwithstanding that a Migration Authorisation in respect of the SMETS1 Installation that includes that Dormant GSME is deemed to have been provided pursuant to Clause 4.27.

5.8C For each SMETS1 Installation where the GSME is an Active Meter and:

(a) where GroupID = “AA”, “BA”, or “CA”; and

(b) the Payment Mode (with its SMETS1 meaning) of the Gas Meter is set to Credit Mode (with its SMETS1 meaning);

then the Responsible Supplier for the SMETS1 GSME may instruct the DCC to exclude the SMETS1 GSME from the SMETS1 Installation in the generation of subsequent Migration Common File(s), notwithstanding that an authorisation may be provided via the Migration Authorisation Mechanism by the Responsible Supplier in respect of a SMETS1 Installation which includes within it the Active GSME. Such instruction shall be provided via a Request to Exclude that complies with Clause 5.8D (a) to (d).

5.8D The following shall apply in respect of a Request to Exclude provided pursuant to Clause 5.8C:

(a) it shall be provided to the DCC using the file exchange arrangements set out in Clause 9 in a reasonable electronic file format notified by the DCC;

(b) it shall be provided to the DCC no later than 10.00 hours on the Wednesday prior to the Migration Week and shall only be applicable to that Migration Week;

(c) it shall overwrite any prior Request to Exclude provided by that Responsible Supplier for that Migration Week;

(d) it may be empty;

(e) the DCC shall disregard any entry in the Request to Exclude where the Responsible Supplier providing the Request to Exclude is not the Responsible Supplier for the Smart Metering System of which the GSME identified in the entry forms a part; and

(f) upon receipt of the final Request to Exclude for a Migration Week, the DCC shall check its contents and shall disregard any entry in it where a change of supplier event is pending in respect of the Smart Metering System of which the GSME identified in the entry forms a part.

5.8E For GroupID = “AA”, “BA”, or “CA”, where, pursuant to Clause 5.8D, a SMETS1 GSME is to be excluded from the preparation of the Migration Common File data for a SMETS1 Installation:

(a) prior to undertaking the check in Clause 5.8F, the DCC shall configure the SMETS1 GPF to prevent any messages from the SMETS1 GSME being sent to the S1SP following Migration; and

(b) the Responsible Supplier for such SMETS1 GSME authorises the DCC to take the steps and carry out the processing specified in Clause 5.8E (a).

5.8F For GroupID = "AA", "BA", or "CA", notwithstanding that an authorisation has been provided (via the Migration Authorisation Mechanism and/or deemed to have been provided pursuant to Clause 4.27) by the Responsible Supplier in respect of a SMETS1 Installation, prior to preparation of the Migration Common File where a SMETS1 GSME is to be excluded from the preparation of the Migration Common File data for a SMETS1 Installation and where the Payment Mode (with its SMETS1 meaning) of the Gas Meter that forms part of that SMETS1 Installation is set to Prepayment Mode (with its SMETS1 meaning), the DCC shall:

(a) exclude the SMETS1 Installation from the preparation of the Migration Common File data; and

(b) configure the SMETS1 GPF to allow any messages from the SMETS1 GSME to be sent to the S1SP.

5.9 Where the DCC receives a Migration Common File, the DCC shall, as the Authenticator, undertake, using whichever parts of the DCC Live Systems it chooses, the sequence of checks and processing required by Table 5.9 for such a file.

Step number	Checks and processing
	Should any of the following checks fail, the Authenticator shall cease processing that file, discard it and raise an Incident.
5.9.1	Confirm the xml file is well formed and valid against the SMETS1 Migration Schema and meets the requirements of Clause 10.1
5.9.2	Check Cryptographic Protection in terms of the signature within the file
5.9.3	Confirm the Remote Party Role specified in the Certificate which was used to Check Cryptographic Protection at Step Number 2 aligns to that required by Table 5.5 for the relevant file type
5.9.4	Confirm Validity of the Certificate used to Check Cryptographic Protection at Step Number 2
5.9.5	Where the file is a Migration Common File confirm either that: 1. the Authenticator holds one or more Migration Common File Stored Counters for the Requesting Party Identifier (RequestingPartyID) and the MCFCounter is not equal to any such Migration Common File Stored Counter created in the last 60 days; or 2. the Authenticator does not hold any Migration Common File Stored Counter for this Requesting Party Identifier Should this check succeed, the Authenticator shall: 1. Create a Migration Common File Stored Counter that is set to the value of MCFCounter
5.9.6	Where the file is a Migration Group File confirm either that: 1. the Authenticator holds one or more Migration Group File Stored Counters for this Requesting Party Identifier (RequestingPartyID) and the MGFCounter is not equal to any such Migration Group File Stored Counter created in the last 60 days; or 2. the Authenticator does not hold a Migration Group File Stored Counter for this Requesting Party Identifier (RequestingPartyID) Should this check succeed, the Authenticator shall: 1. Create a Migration Group File Stored Counter that is set to the value of MGFCounter.

Step number	Checks and processing
5.9.7	Where the file is a Migration Group Encrypted File confirm either that: 1. the Authenticator holds one or more Migration Group Encrypted File Stored Counters for this Requesting Party Identifier (RequestingPartyID) and the MEFCounter is not equal to any such Migration Group Encrypted File Stored Counter created in the last 60 days; or 2. the Authenticator does not hold a Migration Group Encrypted File Stored Counter for this Requesting Party Identifier (RequestingPartyID) Should this check succeed, the Authenticator shall: 1. Create a Migration Group Encrypted File Stored Counter that is set to the value of MEFCounter.
5.9.8	Where the file is a Migration Common Validation File confirm either that: 1. the Authenticator holds one or more Migration File Common Validation Stored Counters for this Requesting Party Identifier (RequestingPartyID) and the MVFCounter is not equal to any such Migration File Common Validation Stored Counter created in the last 60 days; or 2. the Authenticator does not hold a Migration File Common Validation Stored Counter for this Requesting Party Identifier (RequestingPartyID) Should this check succeed, the Authenticator shall: 1. Create a Migration File Common Validation Stored Counter that is set to the value of MVFCounter.
5.9.9	Where the file is a S1SP Commissioning File confirm either that: 1. the Authenticator holds one or more S1SP Commissioning File Stored Counters for this S1SP Identifier (S1SPID) and the SCFCounter is not equal to any such S1SP Commissioning File Stored Counter created in the last 60 days; or 2. the Authenticator does not hold a S1SP Commissioning File Stored Counter for this S1SP Identifier (S1SPID) Should this check succeed, the Authenticator shall: 1. Create a S1SP Commissioning File Stored Counter that is set to the value of SCFCounter.
5.9.10	NOT USED.

Table 5.9

5.10 Where all checks and processing at Clause 5.9 succeed for a Migration Common File, the DCC shall, using whichever parts of the DCC Live Systems it chooses:

(a) ensure that the file is provided to the relevant S1SP, the relevant DCO, and, where ‘ToBeCommissionedByDCC’ is set to ‘True’, the Commissioning Party and, where ‘ToBeCommissionedByDCC’ is set to ‘False’, the Responsible Supplier for the SMETS1 Installations identified with that file over the SMETS1 Migration Interface subject to the naming requirement at Clause 10.2;

(b) create a Migration Common Validation File with the Migration Header having the same values as that of the Migration Common File;

(c) for each SMETS1Installation detailed in the Migration Common File, add a SMETS1Installation element to the Migration Common Validation File where the DeviceID element within the CHF element is that of the SMETS1 CHF of the SMETS1 Installation, and undertake the full sequence of checks and processing in Table 5.10. Should one of those checks fail for a SMETS1 Installation, the DCC shall append to the SMETS1Installation element, a FailedCheck element which includes (1) the relevant StepNumber from Table 5.10 (the ‘FailedStepNumber’) and (2) the SupportingData (as required by the relevant row in from Table 5.10). For clarity, the DCC shall undertake all checks from Table 5.10 for the SMETS1

Installation and so there may be zero, one or many FailedCheck elements for a SMETS1Installation element; and

(d) once all checks are completed for all SMETS1 Installations in the Migration Common File, Digitally Sign the Migration Common Validation File, ensure the relevant S1SP and the relevant DCO has that file, and send that file to the Requesting Party identified by RequestingPartyID.

StepNumber	Check and processing	SupportingData
5.10.1	For the CHF then the ESME then the GSME (if present) and then the PPMID (if present), confirm that the DeviceDetail specified equates to at least one entry on the Central Products List and that that CPL entry is for the required DeviceType	DeviceID of the Device whose Device Model is not on the CPL
5.10.2	For the CHF then the ESME then the GSME (if present) and then the PPMID (if present), confirm that the DeviceDetail specified is one allowable for the GroupID according to the Group Device Model Combination List.	DeviceID of the Device whose Device Model is not within the Group specified by the GroupID
5.10.3	Confirm there is at least one entry on the SMETS1 Eligible Product Combinations which has the combination of Device Models and Device Types specified for this SMETS1 Installation in relation to its CHF, ESME, GSME (if present) and PPMID (if present) and, for at least one such entry the GroupID matches the GroupID in the file.	None
5.10.4	For the CHF then the GPF then the ESME then the GSME (if present) then the PPMID (if present) then the IHD (if present) then the CAD (if present), confirm that DeviceID is not already recorded for any Device in the Smart Metering Inventory.	DeviceID of the Device which is already recorded in the Smart Metering Inventory.
5.10.5	Except for any where the value of CertificateID is the Null Certificate ID, for the ESME, Confirm Validity of each of the Certificates identified by each of the associated four CertificateIDs.	CertificateID for the invalid Certificate
5.10.6	Except for any where the value of CertificateID is the Null Certificate ID, for the GPF, Confirm Validity of each of the Certificates identified by each of the associated four CertificateIDs.	CertificateID for the invalid Certificate
5.10.7	Except for any where the value of CertificateID is the Null Certificate ID, for the GSME if present, Confirm Validity of each of the Certificates identified by each of the associated two CertificateIDs.	CertificateID for the invalid Certificate
5.10.8	Unless the value of the CriticalSupplierCertificateID is the Null Certificate ID for the ESME, confirm, using the Certificates identified by the ESME's CriticalSupplierCertificateID and NonCriticalSupplierCertificateID: • Neither the Critical Supplier ID nor the Non-Critical Supplier ID has the null value; and • the Critical Supplier ID and the Non-Critical Supplier ID identify the same Supplier Party (which is referred to as the 'ESME Supplier Party' in later steps in this Table).	CriticalSupplierCertificateID || NonCriticalSupplierCertificateID
5.10.9	Unless the value of the CriticalSupplierCertificateID is the Null Certificate ID for the ESME, confirm, that, according to Registration Data, the 'ESME Supplier Party' is the current Import Supplier in relation to the MPxN specified in the ESME element.	CriticalSupplierCertificateID
5.10.10	Unless the value of the CriticalSupplierCertificateID is the Null Certificate ID for the ESME, confirm, that, according to Registration Data, there is no change within the next 9 Working Days to the Import Supplier in relation to the MPxN specified in the ESME element.	
5.10.11	Unless the value of the CriticalNetworkOperatorCertificateID is the Null Certificate ID for the ESME, confirm, using the Certificates identified by the ESME's CriticalNetworkOperatorCertificateID and NonCriticalNetworkOperatorCertificateID: • Neither the Critical Network Operator ID nor the Non-Critical Network Operator ID has the null value; and • the Critical Network Operator ID and the Non-Critical Network Operator ID identify the same Network Party (which is referred to as the 'ESME Network Party' in later steps in this Table).	CriticalNetworkOperatorCertificateID || NonCriticalNetworkOperatorCertificateID:
5.10.12	Unless the value of the CriticalNetworkOperatorCertificateID is the Null Certificate ID for the ESME, confirm, that, according to Registration Data, the 'ESME Network Party' is the current Electricity Distributor in relation to the MPxN specified in the ESME element.	CriticalNetworkOperatorCertificateID

StepNumber	Check and processing	SupportingData
5.10.13	If GSME is present, unless the value of the CriticalSupplierCertificateID is the Null Certificate ID for the GSME, confirm, using the Certificates identified by the GSME's CriticalSupplierCertificateID, the GSME's NonCriticalSupplierCertificateID, the GPF's CriticalSupplierCertificateID, and the GPF's NonCriticalSupplierCertificateID: • Neither the Critical Supplier IDs nor the Non-Critical Supplier IDs have the null value; and • the Critical Supplier IDs and the Non-Critical Supplier IDs identify the same Supplier Party (which is referred to as the 'Gas Supplier Party' in later steps in this Table).	CriticalSupplierCertificateID || NonCriticalSupplierCertificateID
5.10.14	Unless the value of the CriticalSupplierCertificateID is the Null Certificate ID for the GSME, confirm, that, according to Registration Data, the 'Gas Supplier Party' is the Gas Supplier in relation to the MPxN specified in the GSME element.	CriticalSupplierCertificateID
5.10.15	Unless the value of the CriticalSupplierCertificateID is the Null Certificate ID for the GSME, confirm, that, according to Registration Data, there is no change within the next 9 Working Days to the Gas Supplier in relation to the MPxN specified in the GSME element.	
5.10.16	Unless the value of the CriticalNetworkOperatorCertificateID is the Null Certificate ID for the GPF, confirm, using the Certificates identified by the GPF's CriticalNetworkOperatorCertificateID and NonCriticalNetworkOperatorCertificateID: • Neither the Critical Network Operator ID nor the Non-Critical Network Operator ID has the null value; and • the Critical Network Operator ID and the Non-Critical Network Operator ID identify the same Network Party (which is referred to as the 'Gas Network Party' in later steps in this Table).	CriticalNetworkOperatorCertificateID || NonCriticalNetworkOperatorCertificateID:
5.10.17	Unless the value of the CriticalNetworkOperatorCertificateID is the Null Certificate ID or the Gas Transporter is an independent Gas Transporter, for the GPF, confirm, that, according to Registration Data, the Gas Network Party is the Gas Transporter in relation to the MPxN specified in the GSME element.	CriticalNetworkOperatorCertificateID
5.10.18	For each of the IHD and CAD, confirm the DeviceType element within the DeviceDetail has the required value.	DeviceID of the Device.

Table 5.10

5.11 Where the Requesting Party, the S1SP or the DCO receives a Migration Common Validation File, it shall, as the Authenticator, undertake the sequence of checks and processing required by Table 5.9 for such a file.

Preparing to trigger Migration

5.12 Where a Requesting Party wishes to Migrate one or more SMETS1 Installations (the 'Requested Installations'), and is in receipt of the required Migration Authorisations for the Requested Installations (or is deemed to have received them pursuant to Clause 4.27 or the definition of Migration Authorisation), the Requesting Party shall first:

(a) confirm a Migration Common File including the Requested Installations has been submitted to the DCC and authenticated as required by Clause 5.8, and a corresponding Migration Common Validation File has been received within the prior 24 hours and authenticated as required by Clause 5.11;

(b) confirm that in the Migration Common Validation File, no errors were detailed for the

Requested Installations;

(c) confirm that there has been one or more wide area network communications with the Communications Hub in each of the Requested Installations within the last 7 days;

(d) where the relevant SMSO is reasonably aware that the Responsible Supplier (or, in the case of Dormant Meters and any associated Devices within the same SMETS1 Installation for which the same Supplier Party is the Responsible Supplier, the DCC) intends to configure any Device within any Requested Installation in accordance with the requirements of the SMETS1 Supporting Requirements (in whole or in part), check that the SMETS1 SMSO has sent the necessary instructions to all such Devices within the Requested Installations to give effect to such configuration;

(e) arrange for the SMETS1 SMSO to take the necessary steps to ensure that all Devices within the Requested Installations, and any associated systems, have been configured in line with the requirements notified by the DCC pursuant to Clause 5.1(b) and where such steps are required, confirm that such steps have been undertaken; and

(f) if required by the ‘Migration Group File’ section of this TMAD for the specified GroupID, populate a Migration Group File with details for the Requested Installations required for the specified GroupID, Digitally Sign and then submit it to the DCC, with the Migration Header having the same values as the Migration Common File; and

(g) if required by the ‘Migration Group Encrypted File’ section of this TMAD for the specified GroupID, populate with details for the Requested Installations, Digitally Sign and then submit to the DCC, a Migration Group Encrypted File, with the Migration Header having the same values as the Migration Common File. The EncryptedS1SPGroupInformation and MasterKeyInformation parts of a Migration Group Encrypted File shall be encrypted according to Clause 11 where the Public Keys used are those notified by the DCC pursuant to Clause 5.1(a) for the GroupID in question.

S1SP and DCO receipt of migration data

5.13 Where the DCC receives a Migration Group Encrypted File, the DCC shall ensure that the DCO and the S1SP, corresponding to the GroupID in the file, have that file.

5.14 Where the DCC receives a Migration Group File, the DCC shall ensure the S1SP corresponding to the GroupID in the file, has that file.

DCO processing on receipt of migration data

5.15 Where the DCO receives a Migration Group Encrypted File, the DCO shall, as the Authenticator, undertake the sequence of checks and processing required by Table 5.9 for such a file. The DCO shall then:

(a) attempt to decrypt the MasterKeyInformation parts of the Migration Group Encrypted File according to Clause 11, where the Public Keys used are those published by DCC pursuant to Clause 5.1(a) for the GroupID in question; and

(b) if this step fails, the DCO shall cease processing that file, discard it and raise an Incident.

5.16 When the DCO has authenticated a Migration Group Encrypted File, it shall start a timer. If that timer reaches 192 hours without the S1SP requesting use of any details in that file, the DCO shall discard the file.

5.17 Where the S1SP requests that the DCO uses details in a Migration Group Encrypted File before the 192 hour timer has elapsed, the DCO shall start another timer. When that timer reaches 60 days, the DCO shall discard any details in the Migration Group Encrypted File related to SMETS1 Installations for which the S1SP has not requested any details be used by the DCO.

5.18 When the DCO authenticates the first Migration Common Validation File for a specific DCO Required File Set, pursuant to Clause 5.20, it shall start a timer. If that timer reaches 24 hours without all of the DCO Required File Set being received, the DCO shall discard the files it has received in that DCO Required File Set.

5.19 If, and only if, the DCO receives all of the files in the DCO Required File Set before its corresponding timer reaches 24 hours, it shall identify the set of SMETS1 Installations from that set which it will allow to be processed further (the "**DCO Viable Installations**"). The DCO shall include in the DCO Viable Installations for this DCO Required File Set all the SMETS1 Installations which:

(a) are included in the Migration Common Validation File, the Migration Common File and, if required, the Migration Group Encrypted File;

(b) do not have any FailedCheck elements within the corresponding SMETS1Installation element in the Migration Common Validation File; and

(c) have not failed any of the checks applied by the DCO as required by ‘DCO Migration Group Encrypted File data validation’ for the specified GroupID, as detailed in the Group Specific

Requirements.

5.20 Where the S1SP requests that the DCO uses some details in relation to a SMETS1 Installation, the DCO shall respond to such requests notifying the S1SP of an error unless either:

(a) the SMETS1 Installation is one of the installations in a set of DCO Viable Installations for which the DCO holds the corresponding DCO Required File Set; or

(b) the SMETS1 Installation was one of the installations in a set of DCO Viable Installations for which the DCO held the corresponding DCO Required File Set when it received a notification from the S1SP that the CHF forming part of that SMETS1 Installation was commissioned.

5.21 When processing such requests from the S1SP, the DCO shall treat only information which is (1) for a DCO Viable Installation and (2) in the corresponding Migration Group Encrypted File as Authorised DCO SMETS1 Device Credentials.

S1SP processing on receipt of migration data

5.22 Where the S1SP receives a Migration Common File, a Migration Common Validation File, a Migration Group File or a Migration Group Encrypted File, the S1SP shall, as the Authenticator, undertake the sequence of checks and processing required by Table 5.9 for such a file.

5.23 For a Migration Group Encrypted File where EncryptedS1SPGroupInformation is required for this GroupID, the S1SP shall then:

(a) attempt to decrypt the EncryptedS1SPGroupInformation parts of the Migration Group Encrypted File according to Clause 11, where the Public Keys used are those notified by DCC pursuant to Clause 5.1(a) for the GroupID in question; and

(b) confirm that the plaintext output from decrypting EncryptedS1SPGroupInformation is well formed and valid against the SMETS1 Migration Schema for a DecryptedS1SPGroupInformation structure or DecryptedS1SPDPGroupInformation structure as in Table 11.2.1.

If either step fails, the S1SP shall cease processing that file, discard it and raise an Incident.

5.24 When the S1SP authenticates, pursuant to Clause 5.22, the first Migration Common Validation File, for a specific S1SP Required File Set, it shall start a timer. If that timer reaches 24 hours without all of the S1SP Required File Set being received, the S1SP shall discard the files it has received in that S1SP Required File Set.

5.25 Where the SISP has received all the files in an S1SP Required File Set and has successfully undertaken the checks required by Clause 5.20 in relation to each of the files, the S1SP shall undertake the sequence of checks and processing required by Table 5.25. Where a SMETS1 Installation fails any of those checks, the S1SP shall include details of that SMETS1 Installation's failure in an S1SP Commissioning File and the S1SP shall undertake no further processing in relation to such SMETS1 Installations as part of the processing of that Migration Group File. Only the SMETS1 Installations which pass all of the checks in Table 5.25 shall be included in the set of S1SP Viable Installations for the S1SP Required File Set.

Step number	Check and processing
	Should any of the following checks fail, checking in relation to that SMETS1 Installation shall cease
5.25.1.1	For each CHFIdentifier in the Migration Group File, where one is required for this GroupID, or in the Migration Group Encrypted File, where a Migration Group File is not required for this GroupID, confirm that the Migration Common File contains a CHFIdentifier with the same value
5.25.1.2	For each CHFIdentifier in the Migration Group File, where one is required for this GroupID, or in the Migration Group Encrypted File, where a Migration Group File is not required for this GroupID, confirm that the Migration Common Validation File does not contain a CHFIdentifier with the same value indicating a validation error
5.25.2.X	Undertake the steps required by the 'S1SP Migration Group File data validation' section of this TMAD for the specified GroupID, where X is the Step number value specified in that section
5.25.3.X	Undertake the steps required by the 'S1SP Migration Group Encrypted File data validation' section of this TMAD for the specified GroupID, where X is the Step number value specified in that section

Table 5.25

5.26 The S1SP shall treat only information which is (i) for an S1SP Viable Installation and (ii) in the corresponding Migration Group Encrypted File as Authorised S1SP SMETS1 Device Credentials.

5.27 For each of the S1SP Viable Installations, the S1SP, and where required the DCO, shall:

(a) undertake, in the order specified, the checks and processing required by the 'S1SP / DCO Commissioning of SMETS1 Installation' section of this TMAD for the associated GroupID;

(b) where a SMETS1 Installation fails any of those checks or processing which is flagged as 'Critical':

(i) include details of that SMETS1 Installation's failure in an S1SP Commissioning File;

(ii) where steps are specified at 'Installation Rollback' for this GroupID, undertake the steps specified to allow communications with the SMETS1 Installation via the relevant SMETS1 SMSO; and

(iii) undertake no further processing in relation to that SMETS1 Installation as part of the processing of the 'DCO Required File Set' or 'S1SP Required File Set', and discard information it has stored or derived about that SMETS1 Installation; and

(c) where a SMETS1 Installation completes all checks and processing without any failures flagged as 'Critical':

(i) record or derive all the information it requires in order to maintain communications with the CHF which forms part of that SMETS1 Installation; and

(ii) include details of that SMETS1 Installation's success in an S1SP Commissioning File.

5.28 The S1SP may include details relating to one or more SMETS1 Installations in each S1SP Commissioning File subject to that inclusion not delaying the sending of details related to any one SMETS1 Installation by more than 60 minutes. Whenever the S1SP creates an S1SP Commissioning File, it shall Digitally Sign that file and send that file:

(a) to the Requesting Party identified by RequestingPartyIdentifier; and either:

(b) where, in the corresponding Migration Common File, the 'ToBeCommissionedByDCC' is set to 'True', to the Commissioning Party identified by CommissioningPartyIdentifier; or

(c) where, in the corresponding Migration Common File, the 'ToBeCommissionedByDCC' is set to 'False', to the Responsible Supplier for the Devices referred to in that file over the SMETS1 Migration Interface.

6 Commissioning Requirements

6.1 Where the Commissioning Party receives a Migration Common File or an S1SP Commissioning File, then the Commissioning Party shall, as the Authenticator, undertake the sequence of checks and processing required by Table 5.9 for such a file. Additionally, the Commissioning Party shall check that any Migration Common File has a value for 'ToBeCommissionedByDCC' set to 'True'. If this check fails, the Commissioning Party shall discard the file and cease processing of it.

6.2 Where the checks undertaken pursuant to Clause 6.1 are successful and the file is a Migration Common File, the Commissioning Party shall start a timer. When that timer reaches 60 days or the Commissioning Party has received and processed S1SP Commissioning Files for all SMETS1 Installations in the Migration Common File, the Commissioning Party shall discard the Migration Common File.

6.3 Where the checks undertaken pursuant to Clause 6.1 are successful and the file is an S1SP

Commissioning File, the Commissioning Party shall, in the following sequence:

(a) confirm that it holds a Migration Common File where the Migration Header has the same values as that S1SP Commissioning File. If it does not, processing of the S1SP Commissioning File shall cease, the file shall be discarded and an Incident shall be raised;

(b) confirm that the S1SP Commissioning File contains details of at least one SMETS1 Installation which the S1SP has successfully processed. If it does not, processing of the S1SP Commissioning File shall cease and the file shall be discarded;

(c) for each SMETS1 Installation specified as being successful in the S1SP Commissioning File, confirm that there is a corresponding SMETS1 Installation in the Migration Common File. Should this check fail for any SMETS1 Installation, processing of the S1SP Commissioning File shall cease, the file shall be discarded and an Incident shall be raised; and

(d) for each SMETS1 Installation in each S1SP Commissioning File that successfully passes the checks at Clause 6.3(a), 6.3(b) and 6.3(c):

(i) submit the Commissioning Requests to the DCC, in line with the requirements of Clause 8 (where ‘Target SMETS1 Device’, ‘Other SMETS1 Device’ and ‘RemotePartyRole’ have their Table 6.3 values for the relevant Commissioning Request), as required by Table 6.3 in the sequence specified, using the details from the Migration Common File for that SMETS1 Installation; and

(ii) include details of that SMETS1 Installation’s processing in a Commissioning Outcome File, specifically by including a SMETS1Installation element, where the DeviceID element within the CHF element is that of the SMETS1 CHF of the SMETS1 Installation. Additionally, where there are any errors in relation to ‘StepNumbers’ 6.3.1 to 6.3.20 the Commissioning Party shall append to the SMETS1Installation element, a FailedCheck element which includes the relevant StepNumber from Table 6.3 (the ‘FailedStepNumber’). For clarity (1) the Commissioning Party shall undertake all relevant steps required by Table 6.3 for the SMETS1 Installation and so there may be zero, one or many FailedCheck elements for a SMETS1Installation element; and (2) where the relevant CertificateID is null or a Device is not present, a step cannot produce errors.

StepNumber	Commissioning Request	Only submit if:	Target SMETS1 Device ID	Other SMETS1 Device ID	RemotePartyRole
6.3.1	Device Pre-notification	True	DeviceID in ESME	NA	NA

StepNumber	Commissioning Request	Only submit if:	Target SMETS1 Device ID	Other SMETS1 Device ID	RemotePartyRole
6.3.2	Update HAN Device Log	True	DeviceID in CHF	DeviceID in ESME	NA
6.3.3	Device Pre-notification	If GSME present	DeviceID in GSME	NA	NA
6.3.4	Update HAN Device Log	If GSME present	DeviceID in CHF	DeviceID in GSME	NA
6.3.5	Device Pre-notification	If PPMID present	DeviceID in PPMID	NA	NA
6.3.6	Update HAN Device Log	If PPMID present	DeviceID in CHF	DeviceID in PPMID	NA
6.3.7	Device Pre-notification	If IHD present	DeviceID in IHD	NA	NA
6.3.8	Update HAN Device Log	If IHD present	DeviceID in CHF	DeviceID in IHD	NA
6.3.9	Device Pre-notification	If CAD present	DeviceID in CAD	NA	NA
6.3.10	Update HAN Device Log	If CAD present	DeviceID in CHF	DeviceID in CAD	NA
6.3.11	Request Handover Of DCC Controlled Device	If Supplier Certificate IDs in the ESME element are not null	DeviceID in ESME	NA	Supplier
6.3.12	Request Handover Of DCC Controlled Device	If (GSME present) and (Supplier Certificate IDs in the GSME element are not null)	DeviceID in GSME	NA	Supplier
6.3.13	Commission Device	True	DeviceID in ESME	NA	NA
6.3.14	Commission Device	If GSME present	DeviceID in GSME	NA	NA
6.3.15	Join Service (Non-Critical)	If PPMID present	DeviceID in PPMID	DeviceID in ESME	NA
6.3.16	Join Service (Critical)	If PPMID present	DeviceID in ESME	DeviceID in PPMID	NA
6.3.17	Join Service (Non-Critical)	If GSME present	DeviceID in GSME	DeviceID in GPF	NA
6.3.18	Request Handover Of DCC Controlled Device	If (GSME present) and (Supplier Certificate IDs in the GPF element are not null)	DeviceID in GPF	NA	Supplier
6.3.19	Request Handover Of DCC Controlled Device	If Network Operator Certificate IDs in the ESME element are not null	DeviceID in ESME	NA	NetworkOperator
6.3.20	Request Handover Of DCC Controlled Device	If Network Operator Certificate IDs in the GPF element are not null	DeviceID in GPF	NA	NetworkOperator

Table 6.3

6.4 The Commissioning Party may include details relating to one or more SMETS1 Installations in each Commissioning Outcome File subject to that inclusion not delaying the sending of details related to any one SMETS1 Installation by more than 60 minutes and, where a Supplier Party is identified in the corresponding entries in the Migration Common File, the Supplier Party is the Responsible Supplier for at least one of the Smart Meters in all of the SMETS1 Installations in that file. Whenever the Commissioning Party creates a Commissioning Outcome File, it shall:

(a) ensure the Migration Header has the same values as that of the Migration Common File; and

(b) Digitally Sign that file and send that file to:

(i) the Requesting Party identified by RequestingPartyIdentifier; and

(ii) where one or more Supplier Parties is identified in the corresponding entries in the Migration Common File, each such Supplier Party via the SMETS1 Migration Interface.

6.5 Where an S1SP receives a Commissioning Request that in accordance with, and subject to, Clause 8.1 is to be treated as a 'Commission Device' Service Request (with its DUIS meaning) for a Device communicating via a CHF that it has established communication with pursuant to Clause 5.27, the S1SP shall establish that Device's Device Model using the Smart Metering Inventory and undertake the processing required for such a Device Model according to the S1SP requirements in the SMETS1 Supporting Requirements. Upon successful completion of the required S1SP processing, where the relevant Service Request is a Commissioning Request, the S1SP shall issue an S1SP Alert, populated according to Table 6.5. For clarity, S1SP Alerts are defined in Version 3.0 of the DCC User Interface Specification, therefore a User that has not yet sent a Service Request using Version 3.0 of the DUIS XML Schema shall not receive such S1SP Alerts.

DUIS Data Item	**Value**
RequestID	Shall be the concatenation of: • The Notified Critical Supplier ID, where the S1SP holds such an identifier in relation to the Device or, where the S1SP does not hold such an identifier, a User ID associated with the Responsible Supplier for the Device; • The Business Target ID in the Commissioning Request; and • 1, separated by ":".
DeviceID	The Business Target ID in the Commissioning Request
S1SPAlertCode	S1MC1
AdditionalInformation	Shall be the sequential concatenation of the following data items: • the MPxN that is, according to the Smart Metering Inventory, associated with the Device identified by the DeviceID; • the EUI-64 identifier of the Communications Hub Function associated with the Device identified by the DeviceID; and • only where the Device identified by the DeviceID is a Gas Smart Meter, the EUI-64 identifier of the Gas Proxy Function associated with that Gas Smart Meter; with a colon (":") used a separator between each data item in the concatenation.
DateTime	Any value as set out in Clause 3.9.15.2 in the DCC User Interface Specification
ds: Signature	Any value as set out in Clause 3.9.15.2 in the DCC User Interface Specification

Table 6.5

6.6 Where, in a Migration Common File, the 'ToBeCommissionedByDCC' set to 'False' the Responsible Supplier for the Devices referred to in that file shall undertake those steps necessary (including submitting Service Requests) to achieve an outcome that is equivalent to that which would have been achieved had the Commissioning Party carried out the steps set out in the Clause 6 in relation to those Devices.

6.7 The S1SP for GroupID = "DA" shall not process any request, received via its interface with the SMETS1 SMSO for that GroupID, to communicate with or generate instructions for a Device in relation to which the steps in Clause 5.12(e) have been carried out, except pursuant to Clause 3.14D.

7 Decommissioning of a Requesting Party or the Commissioning Party

7.1 The DCC shall develop a number of timetables each setting out a date (each a proposed "**RP Decommissioning Date**") at which it proposes to decommission a Requesting Party, each timetable being a draft of a "**RP Decommissioning Timetable**" for the relevant Requesting Party. The DCC shall include within each RP Decommissioning Timetable:.

(a) the final date for which a Migration Authorisation can be submitted (or deemed to be submitted pursuant to Clause 4.27) in respect of the relevant Requesting Party; and

(b) the final Migration Week applicable to the SMETS1 SMSO of which that Requesting Party forms a part.

7.2 Where GroupID = "DA" and "EA", the date within any draft timetable upon which it is proposed to decommission any particular Requesting Party shall be no earlier than twelve months after the date upon which the SMETS1 Eligible Product Combinations is updated by the DCC so as to include an entry for each of the Device Model combinations contained within each Group that pertains to that Requesting Party.

7.3 The DCC shall develop and consult on each RP Decommissioning Timetable (and such consultation may take place prior 10 June 2022). For the purposes of such consultation, the DCC may consult on a date or range of dates that are candidates for the RP Decommissioning Timetable, however the timetable submitted to the Secretary of State must include only one of those dates. The DCC shall consult upon an RP Decommissioning Timetable and submit it to the Secretary of State for approval in accordance with the following process:

(a) the DCC shall, in consultation with Supplier Parties and such other persons as are likely to be interested, produce a draft of the document;

(b) where a disagreement arises with any Supplier Party with regard to any proposal as to the content of the document, the DCC shall endeavour to reach an agreed proposal with that person consistent with the purposes of that RP Decommissioning Timetable;

(c) the DCC shall send a draft of the RP Decommissioning Timetable to the Secretary of State as soon as is practicable after completion of the process described in (a) and (b) above, and shall when doing so provide to the Secretary of State:

(i) a statement of the reasons why the DCC considers that draft to be fit for purpose;

(ii) copies of the consultation responses received; and

(iii) a summary of any disagreements that arose during consultation and that have not been resolved by reaching an agreed proposal; and

(d) the DCC shall comply with any requirements in a direction given to it by the Secretary of State in relation to the draft document.

7.4 Following approval of a RP Decommissioning Timetable by the Secretary of State in accordance with Clause 7.3, the DCC shall publish such RP Decommissioning Timetable to all Supplier Parties and send a copy of the final document to the Secretary of State and to the Authority.

7.4A Following approval of a RP Decommissioning Timetable by the Secretary of State, the DCC shall not take any further step under Clause 4 that relates to a SMETS1 Installation for which it considers commencement of Migration by the relevant Requesting Party could not take place before the expiry of the RP Decommissioning Date for that Requesting Party.

7.5 The DCC may update each RP Decommissioning Timetable by following the procedure in Clause 7.3, provided that the DCC must ensure that the most up to date RP Decommissioning Timetable for each Requesting Party is published to all Supplier Parties and a copy is provided to the Secretary of State and to the Authority.

7.6 Following the expiry of the RP Decommissioning Date for a Requesting Party, the DCC shall ensure that that the relevant Requesting Party does not take any further step under this Code that could result in, or contribute towards, the commencement of Migration for any SMETS1 Installation.

7.7 As soon as reasonably practicable following the RP Decommissioning Date for a Requesting Party, the DCC shall submit a Certificate Revocation Request for all Organisation Certificates in which:

(a) that Requesting Party is identified by the Entity Identifier of the subject of that Organisation Certificate; and

(b) any S1SP that pertains to any Group that pertains to that Requesting Party is identified by the Entity Identifier of the subject of that Organisation Certificate and where such Organisation Certificates have a Remote Party Role of 's1SPMigrationSigning'.

7.8 The DCC shall, as soon as reasonably practicable following the revocation of each of the Organisation Certificates referred to in Clause 7.7, destroy the Private Key associated with each such Organisation Certificate and any associated cryptographic material.

7.9 The DCC shall as soon as reasonably practicable after the RP Decommissioning Date for a Requesting Party:

(a) destroy any Secret Key Material in addition to that referred to in Clause 7.7; and

(b) revoke any Certificate associated with any other Public Key in addition to those referred to in Clause 7.7.

7.9A Following the RP Decommissioning Date for a Requesting Party and in respect of Data that is (in each case) held within any part of the DCC Systems and that was used (or was intended for use) for the purpose of the Migration of the SMETS1 Installations that pertained to that Requesting Party:

(a) the DCC shall retain such Data where it is required for the purposes of providing ongoing Services under the Code in relation to the Devices comprising those SMETS1 Installations and / or where it is required to be retained under the DCC's Data Retention Policy; and

(b) subject to Clause 7.9C, the DCC shall delete such Data where it is not required for the purposes of providing ongoing Services under the Code in relation to the Devices comprising those SMETS1 Installations and / or where it is not required to be retained under the DCC's Data Retention Policy.

7.9B Once the DCC reasonably knows of the date from which it shall no longer require particular Data for the purposes of providing ongoing Services under the Code and / or where it shall no longer require particular Data to be retained under the DCC's Data Retention Policy, the DCC shall promptly notify the Secretary of State and the Authority of the planned date for deletion of the Data and the associated Requesting Party. The planned date within such notification shall be no sooner than 2 months from the date of the notification.

7.9C As soon as reasonably practicable following expiry of the planned date for Data deletion as notified under Clause 7.9B, the DCC shall delete any Data which is the subject of the notice unless either the Secretary of State or the Authority direct that the data should be retained until a later date. Where:

(a) either the Secretary of State or the Authority direct that the Data should be retained until a later date then that Data shall be so retained, or

(b) both the Secretary of State and the Authority direct that the Data should be retained until a later date, the DCC shall retain the Data until the later of the two dates,

and the DCC shall delete the Data as soon as reasonably practicable thereafter.

7.9D The DCC shall as soon as reasonably practicable following each deletion of data pursuant to Clause 7.9C provide the SMKI PMA and the DCC Independent Security Assurance Service Provider with confirmation that the appropriate steps were taken as pursuant to Clause 7.9C.

7.10 As soon as reasonably practicable following the last RP Decommissioning Date the DCC shall submit a Certificate Revocation Request for all Organisation Certificates that identify the Commissioning Party by the Entity Identifier of the subject of those Organisation Certificates.

7.11 The DCC shall, as soon as reasonably practicable following the revocation of each of the Organisation Certificates referred to in Clause 7.10, destroy the Private Key associated with each such Organisation Certificate and any associated cryptographic material.

7.12 The DCC shall as soon as reasonably practicable after the last RP Decommissioning Date:

(a) destroy any Secret Key Material in addition to that referred to in Clause 7.10;

(b) revoke any Certificate associated with any other Public Key in addition to those referred to in Clause 7.10; and

(c) delete any Data,

that (in each case) is held within any part of the DCC Systems and that was used (or was intended for use) for the purpose of the operation of the Commissioning Party; provided that information may be retained for a limited period of time in order to resolve any disagreements over the process.

7.13 The DCC shall as soon as reasonably practicable following the decommissioning of any Requesting Party or the Commissioning Party, obtain an independent audit and provide to the SMKI PMA the report of that audit, confirming that the decommissioning has been properly and successfully carried out together with any remediation plan that may be required.

7.14 Prior to the decommissioning of the Requesting Party, the DCC shall apply the configurations as required by ‘Post Migration Configuration’ for the specified GroupID.

8 Commissioning Requests

8.1 The Commissioning Party and the DCC shall process Commissioning Requests as if they were Service Requests except as varied in this Clause 8.

8.2 The DCC shall not apply any checks on Commissioning Requests that relate to User Role.

8.3 The DCC shall not apply any checks on Commissioning Requests that validate the Notified Critical Supplier ID (with its SMETS1 Supporting requirements meaning) against the Business Originator ID (with its DUIS meaning).

8.4 The DCC shall not apply any validation to Commissioning Requests that relate to Registration Data unless such validation is required by this Clause 8.

8.5 The Commissioning Party shall populate the data items in all Commissioning Requests according to Table 8.7.4, using the information from the Migration Common File where required. Where the S1SP receives a Countersigned Service Request which has InstallCode set to ‘00000000000000000000000000000000’, the S1SP shall not take any related action which would or could affect the communications on any HAN.

8.6 The DCC shall apply the validation checks in Table 8.7.1 to all Commissioning Requests that it receives from the Commissioning Party, and shall additionally apply the validation checks in Table 8.7.3 to any Commissioning Request that it receives from the Commissioning Party which is of the type specified in that Table, and the Commissioning Party shall construct

Commissioning Requests accordingly. Where one of the checks required by this Clause 8.6 fails, the DCC shall send a Service Response to the Commissioning Party detailing the relevant Response Code, which shall be interpreted according to Table 8.7.1 or Table 8.7.3 as appropriate to the Response Code. Where the Commissioning Party receives such a Response other than in relation to a 'Request Handover Of DCC Controlled Device', it shall raise an Incident and not continue processing subsequent Commissioning Requests for that SMETS1 Installation until and unless that incident is resolved so as to allow the erroneous requests to be processed without error. Where the Commissioning Party receives such as Response in relation to a 'Request Handover Of DCC Controlled Device', it shall take the actions required by Clause 6.3(d)(ii) and shall continue processing subsequent Commissioning Requests for that SMETS1 Installation.

8.7 The DCC shall apply the checks in Table 8.7.1 and Table 8.7.3 in the sequence they appear in each Table and shall successfully apply all Table 8.7.1 checks before applying checks in Table 8.7.3. The DCC shall cease processing a Commissioning Request at the point that the first check fails, save that it shall send a response detailing the error to the Commissioning Party.

Validation Check	Response Code	Response Code Name	Response code type	Applicable to response types
The combination of values in the Service Reference and Service Reference Variant fields, with their DUIS meanings, is a combination detailed in one of the rows in Table 8.7.2	E48	Commissioning Party is not allowed to use such Service Requests	Error	Acknowledgement
The Remote Party Role in the Certificate used to verify the Digital Signature on the Commissioning Request is that required by Table 5.5.	C2	Wrong Remote Party Role for Commissioning Request	Error	Acknowledgement
The Business Originator ID in the RequestID (with their DUIS meanings) has the same value as the Entity Identifier in the Certificate used to verify the Digital Signature on the Commissioning Request	E100	Commissioning Party identifier mismatch in Commissioning Service Request	Error	Acknowledgement
Where Business Target ID in the RequestID (with their DUIS meanings) refers to a Device, the Devices is, according to the SMI, a SMETS1 Device or a CAD. For clarity, CADs are not specified in any version of SMETS, and so cannot have an associated SMETS version, where CAD has its DUIS meaning.	C4	Target is not a SMETS1 Device	Error	Acknowledgement
Where the Body part of a Commissioning Request, which is not a 'Device Pre-notification', contains a Device ID (with their DUIS meanings), that Device ID is for a SMETS1 Device according to the Smart Metering Inventory	C5	Other Device is not a SMETS1 Device	Error	Acknowledgement

Table 8.7.1

Commissioning Request name	**Service Reference**	**Service Reference Variant**
Request Handover Of DCC Controlled Device	6.21	6.21
Commission Device	8.1	8.1.1
Join Service (Critical)	8.7	8.7.1
Join Service (Non-Critical)	8.7	8.7.2
Update HAN Device Log	8.11	8.11
Device Pre-notification	12.2	12.2

Table 8.7.2

Commissioning Request name	**Validation Check (**With terms having their DUIS meaning, where not defined otherwise)	**Response Code**	**Response Code name**	**Response code type**	**Applicable to response types**
Request Handover Of DCC Controlled Device	If RemotePartyRole is 'supplier' in the Commissioning Request, confirm that the Remote Party Role in all Certificates in ReplacementCertificates is 'supplier'. If RemotePartyRole is 'NetworkOperator' in the request, confirm that the Remote Party Role in all Certificates in ReplacementCertificates is 'networkOperator'.	C062199	Remote Party Role in Certificates different than in request	Error	Acknowledgement
Request Handover Of DCC Controlled Device	Confirm that the Entity Identifiers in all Certificates contained within ReplacementCertificates are identifiers for the same Party.	C062197	Not all identifiers are for the same Party	Error	Acknowledgement
Request Handover Of DCC Controlled Device	If RemotePartyRole is 'Supplier' in the request, confirm that according to: • the Registration Data linking MPxN to current Import Supplier or Gas Supplier, as the context requires; • the MPxN recorded in the Smart Metering Inventory against; the Device identified by Business Target ID in the request; and • the Party identified by the Entity Identifiers in the Certificates, that the Party identified is the current Import Supplier or Gas Supplier for the Device identified.	C062196	Asserted Supplier is not the Supplier	Error	Acknowledgement
Request Handover Of DCC Controlled Device	If RemotePartyRole is 'NetworkOperator' in the request, confirm that according to: • the Registration Data linking MPxN to current Electricity Distributor or Gas Transporter, as the context requires; • the MPxN recorded in the Smart Metering Inventory against; the Device identified by Business Target ID in the request; and • the Party identified by the Entity Identifiers in the Certificates, that the Party identified is the current Electricity Distributor or Gas Transporter for the Device identified.	C062195	Asserted Network Operator is not the Network Operator	Error	Acknowledgement

Table 8.7.3

DUIS Data Item	Commissioning Service Request(s)	Value
Business Originator ID in Request ID	All	A DCC ID allocated by the DCC for use by the Commissioning Party
Business Target ID in Request ID	All except Device Pre-Notification	‘Target SMETS1 Device ID’
Business Target ID in Request ID	Device Pre-Notification	A DCC ID allocated by the DCC
Originator Counter in Request ID	Join Service (Critical)	For each ‘Target SMETS1 Device ID’, a 64-bit unsigned integer with an initial value of 1 that is increased by 1 for each instance of the Commissioning Request
Originator Counter in Request ID	All except Join Service (Critical)	Any value as set out in Clause 5 in SMETS1 Supporting Requirements Document
ExecutionDateTime	All	Never present
RemotePartyRole	Request Handover Of DCC Controlled Device	‘Supplier’ when processing Certificate IDs provided in relation to a Supplier Party role; or ‘NetworkOperator’ when processing Certificate IDs provided in relation to a Network Party role; or
RemotePartyFloorSeqNumber	Request Handover Of DCC Controlled Device	0 (zero)
RemotePartyPrepaymentTopUpFloorSeqNumber	Request Handover Of DCC Controlled Device	0 (zero) for RemotePartyRole = ‘Supplier’ and Device Type = ESME or GSME Otherwise not present.
ReplacementCertificates	Request Handover Of DCC Controlled Device	The Certificates identified by the Certificate IDs specified for this RemotePartyRole
CertificationPathCertificates	Request Handover Of DCC Controlled Device	The Certification Authority Certificates identified in the Certificates included in ReplacementCertificates.
ApplyTimeBasedCPVChecks	Request Handover Of DCC Controlled Device	True
CurrentDateTime	Commission Device	The Commissioning Parties current date-time which shall be within 10 seconds of UTC
TolerancePeriod	Commission Device	0 (zero)
OtherDeviceID	Join Service (Critical) & Join Service (Non-Critical)	‘Other SMETS1 Device ID’
DeviceID	Update HAN Device Log	‘Other SMETS1 Device ID’
RequestType	Update HAN Device Log	‘Add’
JoinTimePeriod	Update HAN Device Log	1 (one)

DUIS Data Item	Commissioning Service Request(s)	Value
ImportMPxN	Update HAN Device Log	For GSME the MPRN specified for the SMETS1 Installation For ESME; the MPAN specified for the SMETS1 Installation.
SecondaryImportMPAN	Update HAN Device Log	Never present
ExportMPAN	Update HAN Device Log	Never present
DeviceID	Device Pre-Notification	'Target SMETS1 Device ID'
DeviceManufacturer	Device Pre-Notification	As specified in relation to the 'Target SMETS1 Device ID'
DeviceModel	Device Pre-Notification	As specified in relation to the 'Target SMETS1 Device ID'
DeviceType	Device Pre-Notification	The device type specified in relation to the 'Target SMETS1 Device ID', so the relevant one of: • ESME • GSME • PPMID • IHD • CAD
SMETSCHTSVersion	Device Pre-Notification	Not present if DeviceType = "CAD'; as specified in the CPL for the Device Model of the Device identified by the 'Target SMETS1 Device ID' otherwise
FirmwareVersion	Device Pre-Notification	As specified in relation to the 'Target SMETS1 Device ID' where present; otherwise omitted from Commissioning Request
ESMEVariant	Device Pre-Notification	Not present unless DeviceType = "ESME'; 'A' otherwise
AssociatedGPFDeviceID	Device Pre-Notification	Never present

Table 8.7.4

8.8 The DCC shall develop and consult on a "Migration Error Handling and Retry Strategy" in accordance with the following process:

(a) the DCC shall, in consultation with Supplier Parties and such other persons as are likely to be interested, produce a draft of the document;

(b) where a disagreement arises with any Supplier Party with regard to any proposal as to the content of the document, the DCC shall endeavour to reach an agreed proposal with that person consistent with the purposes of the Migration Error Handling and Retry Strategy;

(c) the DCC shall publish a draft of the Migration Error Handling and Retry Strategy as soon as is practicable after completion of the process described in (a) and (b) above together with:

(i) a statement of the reasons why the DCC considers that draft to be fit for purpose;

(ii) copies of the consultation responses received (apart from those marked confidential); and

(iii) a summary of any disagreements that arose during consultation and that have not been resolved by reaching an agreed proposal.

8.9 Within 14 days of DCC publishing the draft Migration Error Handling and Retry Strategy pursuant to Clause 8.8 any Supplier Party may refer the document to the Secretary of State whose decision on its contents shall be final and binding. In the absence of any such referral, the draft published by the DCC shall be Migration Error Handling and Retry Strategy.

8.10 Except where the modification to the Migration Error Handling and Retry Strategy is of a minor typographical nature or where the modification has no material effect on the rights or obligations of Parties, the Migration Error Handling and Retry Strategy may be updated following the procedure set out in Clause 8.8 and 8.9, provided that the DCC must ensure that the most up to date Migration Error Handling and Retry Strategy is published to all Supplier Parties.

8.10A Where the modification to the Migration Error Handling and Retry Strategy is of a minor typographical nature or where the modification has no material effect on the rights or obligations of Parties, the DCC shall publish the updated Migration Error Handling and Retry Strategy to all Supplier Parties together with the date on which it intends that the updated Migration Error Handling and Retry Strategy shall come into effect, which shall be not less than 14 days from the date of publication.

9 SMETS1 Migration Interface

9.1 This Clause 9 specifies the technical interface allowing the exchange of files between the DCC and Supplier Parties pursuant to requirements to exchange files in this TMAD.

9.2 For each Supplier Party, the DCC shall detail directory structures in DCC’s Microsoft SharePoint through which that Supplier Party can exchange files.

9.3 The DCC shall securely exchange only those files which are relevant to a Supplier Party with that Supplier Party through DCC’s Microsoft SharePoint.

10 SMETS1 Migration Schema

10.1 This Clause 10 incorporates the SMETS1 Migration Schema, with which the contents of files created pursuant to this TMAD shall comply, if they are to be valid and authentic. For each file type, the contents shall be a single instance of the XML structure specified in Table 10.2. Each such XML structure shall be populated with information, within each element, as required by Table 10.1 in the format specified by the SMETS1 Migration Schema embedded below.

SMETS1 Migration
Schema v1.2_MOC_F

XML Element	Information
CHFDetail	The information required in relation the SMETS1 CHF which forms part of this SMETS1 Installation and which is required in order to carry out the checks and processing in this TMAD. As per the SMETS1 Migration Schema, this shall not contain any of: • CriticalNetworkOperatorCertificateID • NonCriticalNetworkOperatorCertificateID • CriticalSupplierCertificateID • NonCriticalSupplierCertificateID
GPFDetail	The information required in relation the SMETS1 GPF which forms part of this SMETS1 Installation and which is required in order to carry out the checks and processing in this TMAD. As per the SMETS1 Migration Schema, this shall contain one and only one of each of: • CriticalNetworkOperatorCertificateID • NonCriticalNetworkOperatorCertificateID • CriticalSupplierCertificateID • NonCriticalSupplierCertificateID Where the SMETS1Installation does not contain a GSME, the values in the above four elements shall be the Null Certificate ID.
ESMEDetail	The information required in relation the SMETS1 ESME which forms part of this SMETS1 Installation and which is required in order to carry out the checks and processing in this TMAD. As per the SMETS1 Migration Schema, this shall contain one and only one of each of: • CriticalNetworkOperatorCertificateID • NonCriticalNetworkOperatorCertificateID • CriticalSupplierCertificateID • NonCriticalSupplierCertificateID

XML Element	Information
GSMEDetail	The information required in relation the SMETS1 GSME which forms part of this SMETS1 Installation and which is required in order to carry out the checks and processing in this TMAD. As per the SMETS1 Migration Schema, this shall contain one and only one of each of: • CriticalSupplierCertificateID • NonCriticalSupplierCertificateID As per the SMETS1 Migration Schema, this shall contain not contain: • CriticalNetworkOperatorCertificateID • NonCriticalNetworkOperatorCertificateID
IHDDetail	The information required in relation the SMETS1 IHD which forms part of this SMETS1 Installation and which is required in order to carry out the checks and processing in this TMAD. As per the SMETS1 Migration Schema, this shall not contain any of: • CriticalNetworkOperatorCertificateID • NonCriticalNetworkOperatorCertificateID • CriticalSupplierCertificateID • NonCriticalSupplierCertificateID
PPMIDDetail	The information required in relation the SMETS1 PPMID which forms part of this SMETS1 Installation and which is required in order to carry out the checks and processing in this TMAD. As per the SMETS1 Migration Schema, this shall not contain any of: • CriticalNetworkOperatorCertificateID • NonCriticalNetworkOperatorCertificateID • CriticalSupplierCertificateID • NonCriticalSupplierCertificateID
CADDetail	The information required in relation the SMETS1 CAD which forms part of this SMETS1 Installation and which is required in order to carry out the checks and processing in this TMAD. As per the SMETS1 Migration Schema, this shall not contain any of: • CriticalNetworkOperatorCertificateID • NonCriticalNetworkOperatorCertificateID • CriticalSupplierCertificateID • NonCriticalSupplierCertificateID
DeviceDetail	For the Device to which this element relates, the combination of FirmwareVersion, DeviceModel, DeviceManufacturer (so equating to Device Model) and DeviceType (equating to Device Type)
FirmwareVersion	For the Device to which this element relates, the value required by DUIS in the FirmwareVersion element
DeviceType	For the Device to which this element relates, the value required by DUIS in the DeviceType element
DeviceModel	For the Device to which this element relates, the value required by DUIS in the DeviceModel element
DeviceManufacturer	For the Device to which this element relates, the value required by DUIS in the DeviceManufacturer element
DeviceID	The Device ID of the Device to which this element relates
RequestingPartyID	The DCC ID of the relevant Requesting Party which shall have the same value as Entity Identifier in the Organisation Certificate identified in the X509IssuerSerial element in the file.
S1SPID	The DCC ID of the relevant S1SP which shall have the same value as Entity Identifier in the Organisation Certificate identified in the X509IssuerSerial element in the file.

XML Element	Information
CommissioningPartyID	The DCC ID of the Commissioning Party which shall have the same value as Entity Identifier in the Organisation Certificate identified in the X509IssuerSerial element in the file.
GroupID	The GroupID for the set of SMETS1 Installations detailed in this file.
CriticalNetworkOperatorCertificateID	Where no Network Party is identified, the Null Certificate ID; otherwise a Certificate ID identifying a Certificate which contains the Critical Network Operator ID
NonCriticalNetworkOperatorCertificateID:	Where no Network Party is identified, the Null Certificate ID; otherwise a Certificate ID identifying a Certificate which contains the Non-Critical Network Operator ID
CriticalSupplierCertificateID:	Where no Supplier Party is identified, the Null Certificate ID; otherwise a Certificate ID identifying a Certificate which contains the Critical Supplier ID
NonCriticalSupplierCertificateID:	Where no Supplier Party is identified, the Null Certificate ID; otherwise a Certificate ID identifying a Certificate which contains the Non-Critical Supplier ID
SMETS1Installation	The information required in relation to a SMETS1 Installation in order to carry out the checks and processing in this TMAD.
X509IssuerSerial	In relation to the Signature element, the Certificate ID, which is composed of the X509SerialNumber and X509IssuerName, of the Organisation Certificate that can be used to verify the SignatureValue. In other uses, contains the Certificate ID of the relevant Certificate.
X509SerialNumber	Contains the serialNumber (with its Organisation Certificate Policy meaning) of the relevant Certificate
X509IssuerName	Contains the issuerName (with its Organisation Certificate Policy meaning) of the relevant Certificate
MCFCounter	The current value of the Requesting Party's Migration Common File Counter.
MGFCounter	The current value of the Requesting Party's Migration Group File Counter
MEFCounter	The current value of the Requesting Party's Migration Group Encrypted File Counter
MVFCounter	The current value of the DCC's Migration Common Validation File Counter
SCFCounter	The current value of the S1SP's S1SP Commissioning File Counter
COFCounter	The current value of the Commissioning Party's Commissioning Outcome File Counter
FailedCheck	An element detailing the outcome of a failed check undertaken pursuant to this TMAD
FailedStepNumber	An element detailing which check failed
SupportingData	Additional data associated with a failed check
CHFIdentifier	The DeviceID in the CHFDetail
CertificateID	For the Supporting Data in the Table 5.10
CertificatePair	For the Supporting Data in the Table 5.10
EncryptedS1SPGroupInformation	As required by Table 11.2.1
DecryptedS1SPGroupInformation	As required by Table 11.2.1
DeviceCertificate	As required by Appendix B of this TMAD, the device certificate used to establish TLS communications with the CHF encoded in Base64.
EncryptedMasterKey	Either: • A structure containing one EncryptedKey and a list of one of more DeviceIDs identifying which of the ESME, GPF and CHF the corresponding EncryptedKey is the Master Key (with its DLMS COSEM meaning) for; or • A structure containing one EncryptedKey and the DeviceID of the PPMID where the corresponding EncryptedKey is the Master Key (with its DLMS COSEM meaning) for the PPMID.

<table>
<tr><th>XML Element</th><th>Information</th></tr>
<tr><td>Signature</td><td>As required by Clause 5.5, each of the objects in Table 5.5 shall incorporate a Digital Signature (XMLDSig) generated using the Elliptic Curve Digital Signature Algorithm (ECDSA), and a Private Key for which the associated Public Key is included in an Organisation Certificate with the Remote Party Role Code as in the table in Annex A to Section L.

The parameters and algorithms used shall be
<table>
<tr><th>Parameter/Algorithm</th><th>Value</th></tr>
<tr><td>Reference URI</td><td>“”</td></tr>
<tr><td>Transform Algorithm</td><td>http://www.w3.org/2000/09/xmldsig#enveloped-signature</td></tr>
<tr><td>CanonicalizationMethod Algorithm</td><td>http://www.w3.org/2001/10/xml-exc-c14n#</td></tr>
<tr><td>SignatureMethod Algorithm</td><td>http://www.w3.org/2001/04/xmldsig-more#ecdsa-sha256</td></tr>
<tr><td>DigestMethod Algorithm</td><td>http://www.w3.org/2001/04/xmlenc#sha256</td></tr>
</table>
</td></tr>
<tr><td>KeyInfo</td><td>Shall contain an X509IssuerSerial element (in a single X509Data element) which shall identify the Organisation Certificate that can be used to Check Cryptographic Protection</td></tr>
<tr><td>ToBeCommissionedByDCC</td><td>As required by Clause 5.10</td></tr>
<tr><td>PrepayFlag</td><td>As required by Appendix A of this TMAD.</td></tr>
<tr><td>ESMEVariant</td><td>For the Device to which this element relates, the value required by DUIS in the ESMEVariant</td></tr>
<tr><td>ImportMPAN</td><td>For the Device to which this element relates, the value required by DUIS in the ImportMPxN</td></tr>
<tr><td>MPRN</td><td>For the Device to which this element relates, the value required by DUIS in the ImportMPxN</td></tr>
<tr><td>ReportingPartyID</td><td>The DCC ID of the part of the DCC creating the file, which shall have the same value as Entity Identifier in the Organisation Certificate identified in the X509IssuerSerial element in the file.</td></tr>
<tr><td>IMSI</td><td>The international mobile subscriber identity of the SIM Card used in Comms Hub</td></tr>
<tr><td>IPAddr</td><td>The static IP address associated with the SIM identified by IMSI</td></tr>
<tr><td>DNSServer</td><td>The DNS server IP address configured on the SIM identified by IMSI</td></tr>
<tr><td>PingServer</td><td>The ping server IP address configured on the SIM identified by IMSI</td></tr>
<tr><td>PreviousAPN</td><td>The access point name configured for the SIM identified by IMSI</td></tr>
<tr><td>SerialNumbers</td><td>Each string within SerialNumbers is the serial number of the relevant Device</td></tr>
</table>

Table 10.1

10.2 Each file shall be named according to the following requirements:

FileType_RequesterID_MCFCounter_AdditionalID.xml

where:

- MCFCounter have the values as per the content of the files (so in all cases correspond to the Migration Common File which triggered the processing for the SMETS1 Installation(s) detailed in the file); and

- FileType, RequesterID and AdditionalID have the values required by Table 10.2.

Type of file	FileType value	RequesterID value	AdditionalID value	XML structure within file
Commissioning Outcome File	'COF'	Supplier Signifier value from S1SP Commissioning File filename and ReportingPartyID value concatenated using an "_" (underscore).	COFCounter value from the file	CommissioningOutcomes
Migration Common File	'MCF'	RequestingPartyID value from the file when named by the Requesting Party. When the DCC intends to send to the Registered Supplier over the SMETS1 Migration Interface, RequesterID shall be the Supplier Signifier followed by an "_" (underscore) followed by RequestingPartyID value from the file.	Zero	MigrationCommon
Migration Group File	'MGF'	RequestingPartyID value from the file	MGFCounter value from the file	MigrationGroup
Migration Group Encrypted File	'MEF'	RequestingPartyID value from the file	MEFCounter value from the file	MigrationGroupEncrypted
Migration Common Validation File	'MVF'	ReportingPartyID value from the file	MVFCounter value from the file	MigrationValidation
S1SP Commissioning File	'SCF'	Supplier Signifier and ReportingPartyID value from the file concatenated using an "_" (underscore).	SCFCounter value from the file	S1SPOutcomes

Table 10.2

11 File Content Encryption and Decryption

11.1 A Requesting Party shall only have access to any populated EncryptedS1SPGroupInformation and MasterKeyInformation, where required for the specified GroupID, provided by the relevant SMETS1 SMSO, and shall not have access to either the Plaintext or symmetric keys which were used as input to the population of such elements.

11.2 When a SMETS1 SMSO generates a 128 bit symmetric key for use in relation to this Clause 11, the DCC shall ensure that the SMETS1 SMSO;

(a) generates a new such key for each EncryptedS1SPGroupInformation it creates;

(b) generates each such key using random numbers such as to make it computationally infeasible to regenerate the key even with knowledge of when and by means of what equipment it was generated; and

(c) populates each EncryptedS1SPGroupInformation in line with the requirement of Table 11.2.1 and Table 11.2.2.

Terms in Table 11.2.1 shall have the meanings in NIST Special Publication 800-38D November, 2007 (https://csrc.nist.gov/publications/detail/sp/800-38d/final).

Terms in Table 11.2.2 and Table 11.3 shall have the meanings in IETF RFC 8017 (https://tools.ietf.org/html/rfc8017).

Attribute	**Values**
Plaintext	A string containing fully populated DecryptedS1SPGroupInformation where GroupID = “AA”, “BA”, “CA”, “CB” or “DA”, or DecryptedS1SPDPGroupInformation as required where GroupID = “EA” or “EB”.
Algorithm	AES-GCM-128
Key	The number generated pursuant to Clause 11.2
Initialization Vector	0x000000000000000000000000
Additional Authenticated Data	Empty string
ProtectedData within the EncryptedS1SPGroupInformation	Base64 encoded Ciphertext
AuthenticationTag within the EncryptedS1SPGroupInformation	Base64 encoded 128 bit Authentication Tag

Table 11.2.1

Attribute	**Values**
Algorithm	RSAES-OAEP

Label hash	SHA-256
Mask Generation Function	MGF1 with SHA-1 hash
Recipient's RSA public key	As pursuant to Clause 5.1(a)
Message to be encrypted	The number generated pursuant to Clause 11.2.
Label	Empty string
WrappedTransportKey within the EncryptedS1SPGroupInformation	Base64 encoded Ciphertext

Table 11.2.2

11.3 The DCC shall ensure that each SMETS1 SMSO shall populate EncryptedMasterKey element according to Table 11.3

Attribute	**Values**
Algorithm	RSAES-OAEP
Label hash	SHA-256
Mask Generation Function	MGF1 with SHA-256 hash
Recipient's RSA public key	As pursuant to Clause 5.1(a)
Message to be encrypted	Master Key (with its DLMS COSEM meaning) for the Device(s) identified by DeviceID(s) within EncryptedMasterKey
Label	Empty string
EncryptedKey within the EncryptedMasterKey	Base64 encoded Ciphertext
DeviceID(s) within EncryptedMasterKey	The DeviceID of the Devices for which EncryptedMasterKey contains the Master Key with its DLMS COSEM meaning

Table 11.3

11.3B For GroupID = “DA”, the DCC shall ensure that each SMETS1 SMSO shall populate any required EncryptedSUAKey element according to Table 11.3B

Attribute	**Values**
Algorithm	RSAES-OAEP
Hash	SHA-256
Mask Generation Function	MGF1
Recipient's RSA public key	As pursuant to Clause 5.1(a)
Message to be encrypted	The symmetric key required by the DCO to begin controllinginstructions for the Device
Label	Empty string
EncryptedSUAKey within the SUAKeyDetails	Base64 encoded Ciphertext
DeviceType within SUAKeyDetails	The Device Type of the Device being “ESME” or “GSME”.
PublicKey within SUAKeyDetails	The Base64 encoded uncompressed form of the Elliptic Curve P-256 Public Key, corresponding to the Private Key used for signing ephemeral keys during key establishment with DCO. This is the concatenation 0x04 || X || Y, where len(X)=len(Y)=32 bytes for a 256 bits curve.
SerialNumber within SUAKeyDetails	The Device serial number (according to information held by the relevant SMETS1 SMSO) for the Device.

Table 11.3B

11.4 ensure that each SMETS1 SMSO shall populate any WrappedPrepaymentKey element where it is required for the specified GroupID according to Table 11.4.

Terms in Table 11.4 shall have the meanings in IETF RFC 3394 (https://tools.ietf.org/html/rfc3394).

Attribute	**Values**
Plaintext	The PrepaymentKey within ManagementAssociation for the Device
Algorithm	AES Key Wrap
Key	Master Key (with its DLMS COSEM meaning) for the Device
WrappedPrepaymentKey within the ManagementAssociation	Base64 encoded Ciphertext

Table 11.4

11.5 The DCC shall ensure that each SMETS1 SMSO shall, in populating any required EncryptedS1SPGroupInformation and MasterKeyInformation elements to provide them to the Requesting Party, not decrease the security of the Secret Key Material used as input to the formation of the corresponding Plaintext.

11.6 Where the SMETS1 SMSO and Requesting Party exchange information pursuant to this TMAD, the DCC shall ensure that they shall do so in a way which ensures the information cannot be read by any other entity.

12 Requirements specific to GroupID = "AA"

12.1 This Clause 12 specifies the requirements which are specific to processing in relation to SMETS1Installations where GroupID = "AA".

Pre-enrolment Configuration Requirements

12.2 NOT USED

Migration Group Encrypted File

12.3 A Migration Group Encrypted File is required for this GroupID.

S1SP Required File Set

12.4 The S1SP Required File Set consists of one Migration Common File, one Migration Common Validation File, one Migration Group File and one Migration Group Encrypted File, all with the same Migration Header, and so the same GroupID.

DCO Required File Set

12.5 The DCO Required File Set consists of one Migration Common File, one Migration Common Validation File and one Migration Group Encrypted File, all with the same Migration Header, and so the same GroupID.

S1SP Migration Group File data validation

12.6 The checks at Table 12.6 shall be the 'S1SP Migration Group File data validation' for this GroupID.

Step number	Check and processing
	Should the following check fail, checking in relation to that SMETS1 Installation shall cease
12.6.1	Confirm the following are present and populated validly within the entry with the CHFIdentifier for this SMETS1 Installation: • for the CHFDetails: • IMSI • PreviousAPN • SerialNumbers

Table 12.6

DCO Migration Group Encrypted File data validation

12.7 The checks at Table 12.7 shall be the 'DCO Migration Group Encrypted File data validation' for this GroupID.

Step number	Check and processing
	Should any of the following checks fail, checking in relation to that SMETS1 Installation shall cease
12.7.1	Confirm the following are present and populated validly for the entry with the CHFIdentifier for this SMETS1 Installation: • an EncryptedKeyGPF, and EncryptedKey element within the EncryptedMasterKeyand an EncryptedKey element within the EncryptedMasterKey which contains the DeviceID of the ESME

Table 12.7

S1SP Migration Group Encrypted File data validation

12.8 The checks at Table 12.8 shall be the 'S1SP Migration Group Encrypted File data validation' for this GroupID.

Step number	Check and processing
	Should any of the following checks fail, checking in relation to that SMETS1 Installation shall cease

Step number	Check and processing
12.8.1	Confirm the following are present and populated validly within the DecryptedS1SPGroupInformation for the entry with the CHFIdentifier for this SMETS1 Installation: • for each of the DataCollectionAssociation, ExtendedDataCollectionAssociation, ManagementAssociation and FirmwareAssociation within each of the CHFDetails, GPFDetails and ESMEDetails: • AuthenticationKey • EncryptionKey • for the ESMEDetails: • PrepaymentKey
12.8.2	If there is a GSMEIdentifier for this SMETS1 Installation in the Migration Common File, confirm the following are present and populated validly within the DecryptedS1SPGroupInformation for the GSMEDetails within the entry with the CHFIdentifier for this SMETS1 Installation: • PrepaymentKey

Table 12.8

S1SP / DCO Commissioning of SMETS1 Installation

12.9 The checks at Table 12.9 shall be the 'S1SP / DCO Commissioning of SMETS1 Installation' for this GroupID.

StepNumber	Check and processing	Critical?	SupportingData
	Should any of the following checks which are marked 'Critical' fail, checking in relation to that SMETS1 Installation shall cease		
12.9.1.X	The checks and processing required for 'Installing a SMETS1 Electricity Meter' for this GroupID, as specified in Appendix A of this TMAD, shall be undertaken. For clarity, this includes retrieval of the CHF Whitelist. The information returned shall be that used in subsequent steps.	Yes	The error code for any failure that occurs, as defined in Appendix A of this TMAD.
12.9.2.X	Where a GSMEDetail element is present, the checks and processing required for 'Installing a SMETS1 GSME' for this GroupID, as specified in Appendix A of this TMAD, shall be undertaken.	Yes	The error code for any failure that occurs, as defined in Appendix A of this TMAD.
12.9.1.X	The checks and processing required for 'Securing a SMETS1 ESME' for this GroupID, as specified in Appendix A of this TMAD, shall be undertaken.	Yes	The error code for any failure that occurs, as defined in Appendix A of this TMAD.
12.9.3.X	Where a PPMIDDetail element is present, the checks and processing required for 'Installing a SMETS1 PPMID' for this GroupID, as specified in Appendix A of this TMAD, shall be undertaken.	Yes	The error code for any failure that occurs, as defined in Appendix A of this TMAD.
12.9.4	Where the CHF is of a Device Model which requires the ESME Device Identifier to be in the CHF Whitelist, check that the ESME Device Identifier, included in the Migration Common File for this SMETS1 Installation, is included in the CHF Whitelist retrieved at StepNumber 1.	Yes	
12.9.5	Where a GSME Device Identifier is included in the Migration Common File for this SMETS1 Installation, check that that GSME Device Identifier is included in the CHF Whitelist retrieved at StepNumber 12.9.1.	Yes	
12.9.6	Where a PPMID Device Identifier is included in the Migration Common File for this SMETS1 Installation, check that that PPMID Device Identifier is included in the CHF Whitelist retrieved at StepNumber 12.9.1.	Yes	
12.9.7.X	For the CHF identified in the Migration Common File for this SMETS1 Installation, undertake the processing as specified in Appendix A of this TMAD required 'Commission Device (CHF)' processing for this GroupID and confirm it is successful. For clarity, the DCC shall only return a response indicating success if the CHF Smart Metering Inventory Status is successfully set to 'Commissioned'.	Yes	The error code for any failure that occurs, as defined in Appendix A of this TMAD.

Table 12.9

Installation Rollback

12.10 The processing at Table 12.10 shall be the 'Installation Rollback' for this GroupID**.**

Step number	Check and processing
12.10.1	The DCO shall delete any keys and related information it has stored pursuant to Clause 5.27 in relation to this SMETS1 Installation. The DCO shall either successfully delete all such keys and information or raise an Incident if it cannot.
12.10.2	The S1SP shall delete any keys and information it has stored pursuant to Clause 5.27 in relation to this SMETS1 Installation. The S1SP shall either successfully delete all such keys and information or raise an Incident if it cannot.
12.10.3	The S1SP shall take reasonable steps to restore WAN communication between SMETS1 Installation and the relevant SMETS1 SMSO.

Table 12.10

CHF Whitelist

12.11 The CHF Whitelist shall, for this GroupID, include, for each IEEE address either (1) the UTC date-time at which the CHF last communicated with the identified Device or (2) an indication that the CHF has never communicated with the identified Device.

12.12 The CHF Whitelist shall never include Device IDs for a CHF or a GPF and shall always include the Device ID for an ESME.

Post Migration Configuration

12.13 NOT USED.

Migration Group File

12.14 A Migration Group File is required for this Group ID.

Additional File Structure Validation

12.15 A Migration Group Encrypted File is required for this Group ID, and each such file must include EncryptedS1SPGroupInformation and EncryptedMasterKey, and must not include any SUAKeyDetails.

Migration Common File Device Selection Requirements

12.16 NOT USED.

13 Requirements specific to GroupID = “BA”

13.1 This Clause 13 specifies the requirements which are specific to processing in relation to SMETS1Installations where GroupID =”BA”.

Pre-enrolment Configuration Requirements

13.2 NOT USED.

13.3 The DCC shall ensure that each SMETS1 SMSO shall populate the PrepaymentKey within DecryptedS1SPGroupInformation in Migration Group File with the key used for UTRN generation with;

(a) Where it currently holds such a value, that value; or

(b) Where it does not currently hold such a value, a value it generates. It shall generate such values using random numbers such as to make it computationally infeasible to regenerate the values even with knowledge of when and by means of what equipment they were generated.

13.4 The WrappedPrepaymentKey is required for this GroupID and so shall be populated by the SMETS1 SMSO pursuant to Clause 11.4.

Migration Group Encrypted File

13.5 A Migration Group Encrypted File is required for this GroupID.

S1SP Required File Set

13.6 The S1SP Required File Set consists of one Migration Common File, one Migration Common Validation File, one Migration Group File and one Migration Group Encrypted File, all with the same Migration Header, and so the same GroupID.

DCO Required File Set

13.7 The DCO Required File Set consists of one Migration Common File, one Migration Common Validation File and one Migration Group Encrypted File, all with the same Migration Header, and so the same GroupID.

S1SP Migration Group File data validation

13.8 Clause 12.6 shall apply.

DCO Migration Group Encrypted File data validation

13.9 The checks at Table 13.9 shall be the ‘DCO Migration Group Encrypted File data validation’ for this GroupID.

Step number	Check and processing
	Should any of the following checks fail, checking in relation to that SMETS1 Installation shall cease

Step number	Check and processing
13.9.1	Confirm the following are present and populated validly for the entry with the CHFIdentifier for this SMETS1 Installation: • an EncryptedKey element within the EncryptedMasterKey which contains the DeviceID for each of the CHF, the GPF and the ESME

Table 13.9

S1SP Migration Group Encrypted File data validation

13.10 The checks at Table 13.10 shall be the 'S1SP Migration Group Encrypted File data validation' for this GroupID.

Step number	Check and processing
	Should any of the following checks fail, checking in relation to that SMETS1 Installation shall cease
13.10.1	Confirm the following are present and populated validly within the DecryptedS1SPGroupInformation for the entry with the CHFIdentifier for this SMETS1 Installation: • for each of the DataCollectionAssociation, ExtendedDataCollectionAssociation, ManagementAssociation and FirmwareAssociation within each of the CHFDetails, GPFDetails and ESMEDetails: • AuthenticationKey • EncryptionKey

Table 13.10

S1SP / DCO Commissioning of SMETS1 Installation

13.11 Clause 12.9 shall apply.

Installation Rollback

13.12 Clause 12.10 shall apply.

CHF Whitelist

13.13 The CHF Whitelist shall, for this GroupIDs, include, for each IEEE address, either (1) the UTC date-time at which the CHF last communicated with the identified Device or (2) an indication that the CHF has never communicated with the identified Device.

13.14 The CHF Whitelist shall never include Device IDs for a CHF, a GPF or an ESME and shall only include the Device ID for a GSME where that GSME communicates with the GPF using a ZigBee network.

Post Migration Configuration

13.15 NOT USED

Additional File Structure Validation

13.16 Clause 12.15 shall apply.

Migration Common File Device Selection Requirements

13.17 NOT USED.

14 Requirements specific to GroupID = "CA" or "CB"

14.1 This Section 14 specifies the requirements which are specific to processing in relation to SMETS1Installations where GroupID =”CA” or “CB”.

Pre-enrolment Configuration Requirements

14.2 The DCC shall ensure that each SMETS1 SMSO shall take reasonable steps to configure WAN communication between SMETS1 Installation and the relevant S1SP.

14.3 To enable Clause 14.2 for GroupID = “CB”, the DCC shall ensure that the communication services provider takes all reasonable steps to carry out any precursor steps that are necessary to allow the SMETS1 SMSO to configure the WAN in accordance with Clause 14.2 and provide any relevant information to the SMETS1 SMSO.

Migration Group Encrypted File

14.4 A Migration Group Encrypted File is required for these GroupIDs.

S1SP Required File Set

14.5 The S1SP Required File Set consists of one Migration Common File, one Migration Common Validation File, one Migration Group File and one Migration Group Encrypted File, all with the same Migration Header, and so the same GroupID.

DCO Required File Set

14.6 The DCO Required File Set consists of one Migration Common File, one Migration Common Validation File and one Migration Group Encrypted File, all with the same Migration Header, and so the same GroupID.

S1SP Migration Group File data validation

14.7 The checks at Table 14.7 shall be the ‘S1SP Migration Group File data validation’ for these GroupIDs.

Step number	Check and processing
	Should any of the following checks fail, checking in relation to that SMETS1 Installation shall cease
14.7.1	Confirm the following are present and populated validly within the entry with the CHFIdentifier for this SMETS1 Installation: • for the CHFDetails: • IMSI • IPAddr • PreviousAPN • SerialNumbers

Table 14.7

DCO Migration Group Encrypted File data validation

14.8 The checks at Table 14.8 shall be the 'DCO Migration Group Encrypted File data validation' for these GroupIDs.

Step number	Check and processing
	Should any of the following checks fail, checking in relation to that SMETS1 Installation shall cease
14.8.1	Confirm the following are present and populated validly for the entry with the CHFIdentifier for this SMETS1 Installation: • an EncryptedKey element within the EncryptedMasterKey which contains the DeviceID of the CHF, an EncryptedKey element within the EncryptedMasterKey which contains the DeviceID of the GPF and an EncryptedMasterKey element which contains the DeviceID of the ESME

Table 14.8

S1SP Migration Group Encrypted File data validation

14.9 The checks at Table 14.9 shall be the 'S1SP Migration Group Encrypted File data validation' for this GroupID.

Step number	Check and processing
	Should any of the following checks fail, checking in relation to that SMETS1 Installation shall cease
14.9.1	Confirm the following are present and populated validly within the DecryptedS1SPGroupInformation for the entry with the CHFIdentifier for this SMETS1 Installation: • for each of the DataCollectionAssociation, ExtendedDataCollectionAssociation, ManagementAssociation and FirmwareAssociation within each of the CHFDetails, GPFDetails and ESMEDetails: • AuthenticationKey • EncryptionKey

Table 14.9

S1SP / DCO Commissioning of SMETS1 Installation

14.10 Clause 12.9 shall apply.

Installation Rollback

14.11 Clause 12.10 shall apply.

CHF Whitelist

14.12 The CHF Whitelist shall, for this GroupID, include, for each IEEE address either (1) the UTC date-time at which the CHF last communicated with the identified Device or (2) an indication that the CHF has never communicated with the identified Device.

14.13 The CHF Whitelist shall never include Device IDs for a CHF, a GPF or an ESME and shall only include the Device ID for a GSME where that GSME communicates with the GPF using a ZigBee network.

Post Migration Configuration

14.14 For GroupID = “CB”, the DCC shall ensure that the communications services provider takes all reasonable steps to ensure that the SMETS1 SMSO can no longer communicate with the Commissioned SMETS1 Devices or any associated communications service provider systems.

Migration Group File

14.15 A Migration Group File is required for this Group ID.

Additional File Structure Validation

14.16 Clause 12.15 shall apply.

Migration Common File Device Selection Requirements

14.17 NOT USED.

15 Requirements specific to GroupID = "EA" or "EB"

15.1 This Section 15 specifies the requirements which are specific to processing in relation to SMETS1 Installations where GroupID = "EA" or "EB".

Pre-enrolment Configuration Requirements

15.2 Prior to Migration of a SMETS1 Installation where GroupID = "EA" or "EB" the DCC shall ensure that configuration by each SMETS1 SMSO takes place to enable communication between the SMETS1 Installation and relevant S1SP.

Migration Group Encrypted File

15.3 A Migration Group Encrypted File is required for these GroupIDs. Each file must include EncryptedS1SPGroupInformation and EncryptedMasterKey elements.

S1SP Required File Set

15.4 The S1SP Required File Set consists of one Migration Common File, one Migration Common Validation File, one Migration Group File and one Migration Group Encrypted File, all with the same Migration Header, and so the same GroupID.

DCO Required File Set

15.5 The DCO Required File Set consists of one Migration Common File, one Migration Common Validation File and one Migration Group Encrypted File, all with the same Migration Header, and so the same GroupID.

S1SP Migration Group File data validation

15.6 The checks at Table 15.6 shall be the 'S1SP Migration Group File data validation' for these GroupIDs.

Step number	Check and processing
	Should any of the following checks fail, checking in relation to that SMETS1 Installation shall cease
15.6.1	Confirm the following are present and populated validly within the entry with the CHFIdentifier for this SMETS1 Installation: • for the CHFDetails: • IMSI • PreviousAPN

Table 15.6

DCO Migration Group Encrypted File data validation

15.7 The checks at Table 15.7 shall be the 'DCO Migration Group Encrypted File data validation' for these GroupIDs.

Step	Check and processing
	Should any of the following checks fail, checking in relation to that SMETS1Installation shall cease
15.7.1	Confirm the following are present and populated validly for the entry with the CHFIdentifier for this SMETS1 Installation: • an EncryptedKey element within the EncryptedMasterKey which contains the DeviceID of the ESME

Table 15.7

S1SP Migration Group Encrypted File data validation

15.8 The checks at Table 15.8 shall be the 'S1SP Migration Group Encrypted File data validation for these GroupIDs.

Step number	Check and processing
	Should any of the following checks fail, checking in relation to that SMETS1 Installation shall cease
15.8.1	Confirm the following are present and populated validly within the DecryptedS1SPDPGroupInformation for the entry with the CHFIdentifier for this SMETS1 Installation: • for HighLevelAssociation within the ESMEDetail • AuthenticationKey • EncryptionKey • PrepaymentKey
15.8.2	For each GSME identified in the GSMEIdentifier for this SMETS1 Installation in the Migration Common File, confirm the following are present and populated validly within the DecryptedS1SPDPGroupInformation for the GSMEDetail/PrePayDetails within the entry with the CHFIdentifier for this SMETS1 Installation: a. PrepaymentKey

Table 15.8

S1SP / DCO Commissioning of SMETS1 Installation

15.9 The checks at Table 15.9 shall be the 'S1SP / DCO Commissioning of SMETS1 Installation' for these GroupIDs.

StepNumber	Check and processing	Critical?	SupportingData
	Should any of the following checks which are marked 'Critical' fail, checking in relation to that SMETS1 Installation shall cease		
15.9.1.X	The checks and processing required for 'Installing a SMETS1 Electricity Meter' for this Group ID, as specified Appendix B of this TMAD, shall be undertaken. For clarity, this includes retrieval of the CHF Whitelist. The information returned shall be that used in subsequent steps.	Yes	The error code for any failure that occurs, as defined in Appendix B of this TMAD.
15.9.2.X	Where a GSMEDetail element is present, the checks and processing required for 'Installing a SMETS1 GSME' for this Group ID, as specified in Appendix B of this TMAD, shall be undertaken.	Yes	The error code for any failure that occurs, as defined in Appendix B of this TMAD.
15.9.3.X	Where a PPMIDDetail element is present, the checks and processing required for 'Installing a SMETS1 PPMID' for this Group ID, as specified in Appendix B of this TMAD, shall be undertaken.	Yes	The error code for any failure that occurs, as defined in Appendix B of this TMAD.
15.9.4	Where a PPMID Device Identifier is included in the Migration Common File for this SMETS1 Installation, check that that PPMID Device Identifier is included in the CHF Whitelist retrieved at StepNumber 15.9.1.	Yes	
15.9.4a.X	The checks and processing shall be undertaken for 'Configure Pushing of Profile Data' for this Group ID, as specified in Appendix B of this TMAD.	Yes	The error code for any failure that occurs, as defined in Appendix B of this TMAD.
15.9.5.X	The checks and processing required for 'Securing a SMETS1 ESME' for this Group ID, as specified in Appendix B of this TMAD, shall be undertaken.	Yes	The error code for any failure that occurs, as defined in Appendix B of this TMAD.

StepNumber	Check and processing	Critical?	SupportingData
15.9.6.X	For the CHF identified in the Migration Common File for this SMETS1 Installation, undertake the steps set out in Appendix B of this TMAD required 'Commission Device (CHF)' processing for this GroupID and confirm it is successful. For clarity, the DCC shall only return a response indicating success if the CHF Smart Metering Inventory Status is successfully set to 'Commissioned'.	Yes	The error code for any failure that occurs, as defined in Appendix B of this TMAD.

Table 15.9

Installation Rollback

15.10 The processing at Table 15.10 shall be the 'Installation Rollback' for these GroupIDs**.**

Step number	Check and processing
15.10.1	The DCO shall delete any keys and related information it has stored pursuant to Clause 5.27 in relation to this SMETS1 Installation. The DCO shall either successfully delete all such keys and information or raise an Incident if it cannot.
15.10.2	The S1SP shall delete any keys and information it has stored pursuant to Clause 5.27 in relation to this SMETS1 Installation. The S1SP shall either successfully delete all such keys and information or raise an Incident if it cannot.
15.10.3	The S1SP shall take all reasonable steps to re-instate SMSO certificates on Devices.
15.10.4	The S1SP shall take reasonable steps to restore prior WAN communication settings between the SMETS1 Installation and the relevant SMETS1 SMSO.

Table 15.10

16 Requirements specific to GroupID = “DA”

16.1 This Clause 16 specifies the requirements which are specific to processing in relation to SMETS1 Installations where GroupID = “DA”.

Pre-enrolment Configuration Requirements

16.2 NOT USED

Migration Group Encrypted File

16.3 A Migration Group Encrypted File is required for this GroupID.

S1SP Required File Set

16.4 The S1SP Required File Set consists of one Migration Common File, one Migration Common Validation File, and one Migration Group Encrypted File, all with the same Migration Header, and so the same GroupID.

DCO Required File Set

16.5 The DCO Required File Set consists of one Migration Common File, one Migration Common Validation File and one Migration Group Encrypted File, all with the same Migration Header, and so the same GroupID.

S1SP Migration Group File data validation

16.6 NONE REQUIRED.

DCO Migration Group Encrypted File data validation

16.7 The checks at Table 16.7 shall be the ‘DCO Migration Group Encrypted File data validation’ for this GroupID.

Step	Check and processing
	Should any of the following checks fail, checking in relation to that SMETS1 Installation shall cease
16.7.1	For each SMETS1Installation, confirm there are no EncryptedMasterKey elements.
16.7.2	For each SMETS1Installation, confirm there is one and only one EncryptedSUAKey (referring to a SUA Symmetric Key) element with DeviceType of “ESME”.

Step	Check and processing
16.7.3	If according to the "Migration Common File" there is a "GSME" in this SMETS1Installation, confirm there is one and only one other EncryptedSUAKey (referring to a SUA Symmetric Key) element which has a DeviceType of "GSME".
16.7.4	If according to the "Migration Common File" there is no "GSME" in this SMETS1Installation, confirm there is no other EncryptedSUAKey (SUA Symmetric Keys) element.
16.7.5	For each SMETS1Installation, confirm that there is no empty child element within any SUAKeyDetails element.

Table 16.7

S1SP Migration Group Encrypted File data validation

16.8 NONE REQUIRED.

S1SP / DCO Commissioning of SMETS1 Installation

16.9 The steps at Table 16.9 may be carried out by the DCC up to 7 days in advance of the other steps in Clause 5.27 for the SMETS1 Installation in question.

StepNumber	Check and processing	Critical?	SupportingData
	Should any of the following checks which are marked 'Critical' fail, checking in relation to that SMETS1 Installation shall cease		
16.9.1.x	The checks and processing required for 'Installing a SMETS1 Electricity Meter' for this GroupID, as specified in Appendix C of this TMAD, shall be undertaken. For clarity, this includes retrieval of the CHF Whitelist. The information returned shall be that used in subsequent steps.	Yes	The error code for any failure that occurs, as defined in Appendix C of this TMAD.
16.9.2.x	Where a GSMEDetail element is present, the checks and processing required for 'Installing a SMETS1 GSME' for this GroupID, as specified in Appendix C of this TMAD, shall be undertaken.	Yes	The error code for any failure that occurs, as defined in Appendix C of this TMAD.
16.9.3	Where a PPMIDDetail element is present, the checks and processing required for 'Installing a SMETS1 PPMID' for this GroupID, as specified in Appendix C of this TMAD, shall be undertaken.	Yes	The error code for any failure that occurs, as defined in Appendix C of this TMAD.
16.9.4	Where a PPMID Device Identifier is included in the Migration Common File for this SMETS1 Installation, check that that PPMID Device Identifier is included in the CHF Whitelist retrieved at StepNumber 16.9.1.	Yes	

Table 16.9

16.10 The steps at Table 16.10 shall not be carried out in advance of the other steps in Clause 5.27 for the SMETS1 Installation in question.

StepNumber	Check and processing	Critical?	SupportingData
	Should any of the following checks which are marked 'Critical' fail, checking in relation to that SMETS1 Installation shall cease		
16.10.1.X	Where a GSMEDetail element is present, the checks and processing required for 'Securing a SMETS1 GSME' for this GroupID, as specified in Appendix C of this TMAD, shall be undertaken.	Yes	The error code for any failure that occurs, as defined in Appendix C of this TMAD.
16.10.2.X	The checks and processing required for 'Securing a SMETS1 ESME' for this GroupID, as specified in Appendix C of this TMAD, shall be undertaken.	Yes	The error code for any failure that occurs, as defined in Appendix C of this TMAD.

StepNumber	Check and processing	Critical?	SupportingData
16.10.3.X	For the CHF identified in the Migration Common File for this SMETS1 Installation, undertake the checks and processing required for 'Commission Device (CHF)' for this GroupID, as specified in Appendix C of this TMAD, and confirm it is successful. For clarity, the DCC shall only return a response indicating success if the CHF Smart Metering Inventory Status is successfully set to 'Commissioned'.	Yes	The error code for any failure that occurs, as defined in Appendix C of this TMAD.

Table 16.10

Installation Rollback

16.11 The processing at Table 16.11 shall be the 'Installation Rollback' for this GroupID.

Step number	Check and processing
16.11.1	If GSMEDetail is present, the S1SP shall revert control of the SMETS1 Installation to the relevant SMETS1 SMSO where any of the steps in "Securing a SMETS1 GSME" fails for this GroupID . The S1SP shall not revert control of the SMETS1 Installation to the relevant SMETS1 SMSO if any of the steps in "Securing a SMETS1 ESME" fails for this GroupID.

Table 16.11

CHF Whitelist

16.12 The CHF Whitelist shall, for this GroupID, include, for each IEEE address either (1) the UTC date-time at which the CHF last communicated with the identified Device or (2) an indication that the CHF has never communicated with the identified Device.

16.13 The CHF Whitelist shall never include Device IDs for a CHF, a GPF or an ESME and shall only include the Device ID for a GSME where that GSME communicates with the GPF.

Post Migration Configuration

16.14 NOT USED.

Migration Group File

16.15 A Migration Group File is not required for this GroupID.

Additional File Structure Validation

16.16 A Migration Group Encrypted File is required for this GroupID, and each such file must not include any EncryptedS1SPGroupInformation or any EncryptedMasterKey, and must include SUAKeyDetails.

Migration Common File Device Selection Requirements

16.17 Where there is more than one SMETS1 PPMID, SMETS1 IHD or SMETS1 CAD in a SMETS1

Installation that solely comprises Dormant meters, the DCC shall include only one of each Device Type in the Migration Common File, being the one that most recently joined the HAN.

17 SMETS1 Device Security Testing

17.1 The DCC shall carry out SMETS1 Device Security Testing in accordance with the requirements of this Clause 17 for the purpose of identifying security risks to the DCC Total System.

17.2 Each Supplier Party hereby acknowledges that in preparing and conducting SMETS1 Device Security Testing under this Clause 17, the DCC does not warrant or represent that SMETS1 Device Models or combinations of SMETS1 Device Models operate or do not operate in a particular way when comprising part of an Enrolled SMETS1 Smart Metering System.

17.3 No later than 5 Working Days following this Clause 17.3 coming into effect, the DCC shall submit the SMETS1 Device Security Testing Scope and Timetable Document to the Security Sub-Committee (and such submission may take place prior to this this Clause 17.3 coming into effect). The SMETS1 Device Security Testing Scope and Timetable Document shall set out:

(a) the SMETS1 Device Models (and, where relevant, the combinations of SMETS1 Device Models) that are to be the subject of SMETS1 Device Security Testing which shall be those SMETS1 Device Models proposed to the Security Sub-Committee for the purposes of SMETS1 Device Security Testing by the DCC on 14 May 2020;

(b) the nature of the tests (including negative tests) that are to be carried out as part of SMETS1 Device Security Testing, which shall be those tests that were agreed by the Security Sub-Committee for the purposes of SMETS1 Device Security Testing on 8 January 2020; and

(c) the associated reasonable timetable in accordance with which the tests are to be carried out.

17.4 The DCC may seek variations to the SMETS1 Device Security Testing Scope and Timetable Document by submitting a revised draft SMETS1 Device Security Testing Scope and Timetable Document to the Security Sub-Committee for review, provided that the nature of the tests may not be modified so as to result in a material deviation from the implicit purposes of the tests referred to in Clause 17.3(b):

(a) where the Security Sub-Committee and the DCC can reach an agreement, the relevant revised draft SMETS1 Device Security Testing Scope and Timetable Document shall be updated by the DCC as necessary and deemed to be final; or

(b) where the Security Sub-Committee and the DCC cannot reach an agreement, the relevant revised draft SMETS1 Device Security Testing Scope and Timetable Document shall be referred by the DCC to the Secretary of State for determination (whose decision shall be final and binding for the purposes of this Code) and the relevant revised draft SMETS1 Device Security Testing Scope and Timetable Document shall be updated by the DCC as necessary and deemed to be final.

17.5 The DCC shall take reasonable steps to complete the tests set out in the SMETS1 Device Security Testing Scope and Timetable Document in accordance with the timetable set out therein.

17.6 Revisions to the SMETS1 Device Security Testing Scope and Timetable Document finalised pursuant to Clause 17.4 may, from time to time be submitted by the DCC to the Security Sub-Committee in accordance with the provisions of Clause 17.4, and the provisions of Clauses 17.4 and 17.5 shall apply (again) to the revised version of the document.

17.7 The DCC shall take all reasonable steps to obtain a reasonable number of SMETS1 Devices for use in SMETS1 Device Security Testing and necessary consents.

17.8 In order that the DCC may perform SMETS1 Device Security Testing, any Supplier Party that is an Installing Supplier for any of the SMETS1 Device Models identified in the SMETS1 Device Security Testing Scope and Timetable Document shall take all reasonable steps to provide such support and assistance as the DCC may reasonably request including the provision of:

(a) such SMETS1 Devices; and

(b) firmware and firmware upgrades applicable to such SMETS1 Devices in an appropriate format to enable security testing consistent with the SMETS1 Device Security Testing Scope and Timetable Document.

17.9 Each Supplier Party providing SMETS1 Devices pursuant to Clause 17.8 is deemed to have provided consent, or procured consent, for the security testing of such SMETS1 Devices consistent with the SMETS1 Device Security Testing Scope and Timetable Document.

17.10 SMETS1 Device Security Testing shall only be performed by the DCC using SMETS1 Devices which are installed in appropriate DCC appointed test laboratories.

17.11 Where the DCC reasonably considers that any SMETS1 Device Security Testing in relation to a relevant SMETS1 Device Model (or, where relevant, combinations of SMETS1 Device Models) is complete, the DCC shall, as soon as reasonably practicable, provide a report (being a SMETS1 Device Security Testing Completion Report) to the Security Sub-Committee setting out the results of such tests for review by the Security Sub-Committee. Following such review, the DCC shall update each SMETS1 Device Security Testing Completion Report to include any observations provided by the Security Sub-Committee and the DCC’s responses to those observations and that SMETS1 Device Security Testing Completion Report shall be deemed to be final.

17.12 The DCC shall promptly provide each final SMETS1 Device Security Testing Completion Report to the Security Sub-Committee (and copied to the Secretary of State).

18 Excluded Categories

18.1 Where there is any conflict between the other Clauses of this TMAD and this Clause 18, this Clause 18 shall take precedence.

18.2This Clause 18 describes each category of SMETS1 SMS or SMETS1 Installation:

(a) that are not, or will no longer be, eligible for Enrolment and accordingly, will not be Enrolled;

(b) that shall no longer be eligible for Migration notwithstanding that there may be an entry on the EPCL corresponding to such SMETS1 Installation; and/or

(c) for which DCC shall no longer be required to take steps which would enable it to propose an entry to the EPCL which corresponds to such SMETS1 Installation.

Each such category shall be an Excluded Category and any SMETS1 Installation or SMETS1 SMS falling within an Excluded Category shall no longer be treated by the DCC as comprising SMETS1 Meters for which the Secretary of State has concluded that the DCC is required to provide SMETS1 Services and shall no longer be In-Scope for Enrolment.

18.2A Where:

(a) a SMETS1 Installation comprises solely Dormant Meters;

(b) the Responsible Supplier for the SMSs within that SMETS1 Installation (where there is more than one) is the same; and

(c) the Dormant Meters have such a status because the DCC reasonably believes that the Responsible Supplier has terminated its arrangements with the relevant SMETS1 SMSO,

following a request from the DCC, the Responsible Supplier shall promptly provide the DCC with a statement (and provision of such statement may take place prior to this Clause 18.2A and Clause 18.14 coming into effect) that either:

(d) confirms that in its reasonable opinion such SMETS1 Installation is not capable of successfully being Migrated; or

(e) confirms that in its reasonable opinion such SMETS1 Installation may be capable of successfully being Migrated.

18.3 By the last Working Day of each month, the DCC shall provide each Responsible Supplier with information relating to their SMETS1 SMS(s) which comprise all or part of an Excluded Category. Such information shall be provided via the file exchange arrangements set out in Clause 9 and shall include:

(a) the Excluded Category;

(b) for each excluded GSME, the MPRN for the relevant SMETS1 Installation; and

(c) for each excluded ESME, the MPAN for the relevant SMETS1 Installation.

<u>Excluded Category - Master Key Errors</u>

18.4 Clause 18.2 (b) applies for each SMETS1 Installation where:

(a) GroupID = “AA”, “BA”, “CA”, or “CB”;

(b) it comprises solely Dormant Meters; and

the DCC has taken all reasonable steps to obtain the correct Master Key (with its DLMS COSEM meaning) for the SMETS1 CHF within the SMETS1 Installation required to enable the corresponding SMETS1 Installation to be successfully migrated but the DCC has been unable to obtain such correct Master Key (and steps to obtain such correct Master Key may take place prior to this this Clause 18 coming into effect).

<u>Excluded Category - Partial Migration</u>

18.5 Clause 18.2 (a) applies to the SMETS1 GSMS where:

(a) a new Migration Common File (that excludes the SMETS1 GSME) is generated pursuant to Clause 5.8C and 5.8D; or

(b) a Gas Meter is deregistered pursuant to either Clause 4.26A or 4.26B.

<u>Excluded Category – No WAN Before Migration Attempted</u>

18.6 Clause 18.2 (b) applies where:

(a) GroupID = “AA”, “BA”, or “CA”;

(b) a SMETS1 Installation contains solely Dormant Meters;

(c) the DCC has instructed the relevant SMETS1 SMSO to take the steps described in Clause 4.26 at least three times (and each such instruction may take place prior to this this Clause 18 coming into effect); and

(d) each time the steps described in Clause 4.26 have been unsuccessful as the SMETS1 SMSO has been unable to successfully complete the requested firmware upgrade and/or configuration where the failure is attributed by the SMETS1 SMSO as an inability to maintain the wide area network communication with the Communications Hub.

Notwithstanding that Clause 18.2 (b) applies, prior to decommissioning of the Requesting Party for the GroupID (pursuant to Clause 7), the DCC shall instruct the SMETS1 SMSO to re-

attempt the steps described in Clause 4.26 for a SMETS1 Installation for which Clause 18.6 (a) to (d) applies, following the receipt of a request from the Responsible Supplier to do so. In the case of SMETS1 Installations comprising both a GSMS and an ESMS the instruction shall only be actioned by the DCC where the Responsible Supplier for both Smart Metering Systems is the same. The DCC shall commence the Migration of the SMETS1 Installation should the steps required under Clause 4.26 be successfully executed.

<u>Excluded Category – No WAN Attempting Migration</u>

18.7 Clause 18.2 (b) applies where:

(a) GroupID = “AA”, “BA”, “CA”, or “CB”;

(b) the SMETS1 Installation contains solely Dormant Meters;

(c) the DCC has commenced Migration for the SMETS1 Installation at least three times each in separate and non-contiguous Migration Weeks (and each such commencement of Migration may take place prior to this this Clause 18 coming into effect); and

(d) each time the Requesting Party has been unable confirm that there has been one or more wide area network communications with the Communications Hub in the SMETS1 Installation within the last 7 days pursuant to Clause 5.12 (c).

Notwithstanding that Clause 18.2 (b) applies, prior to decommissioning of the Requesting Party (pursuant to Clause 7) the DCC shall re-attempt the Migration of the SMETS1 Installation to which Clause 18.7 (a) to (d) applies, following the receipt of a request from the Responsible Supplier to do so. In the case of SMETS1 Installations comprising both a GSMS and an ESMS the Migration shall only be reattempted by the DCC where the Responsible Supplier for both Smart Metering Systems is the same.

Excluded Category – Five Retries Attempting Migration

18.8 Clause 18.2 (b) applies where:

(a) [NOT USED];

(b) the SMETS1 Installation contains solely Dormant Meter(s);

(c) the DCC has commenced Migration for the corresponding SMETS1 Installation at least five times each in separate Migration Weeks (and each such commencement of Migration may take place prior to this Clause 18 coming into effect);

(d) each time the Migration has failed to complete successfully; and

(e) none of the failures relate to:

(i) a check set out in Table 5.9 or in Table 5.10;

(ii) expiry of a Migration Authorisation;

(iii) the ET02.4.4 check; or

(iv) where GroupID = "EA" and the SMETS1 Installation does not contain a GSME, the GT02.3 or GT01.4 check for a Migration attempt prior to 2 November 2022.

Notwithstanding that Clause 18.2 (b) applies, prior to decommissioning of the Requesting Party (pursuant to Clause 7) the DCC shall re-attempt the Migration of the SMETS1 Installation to which Clause 18.8 (a) to (e) applies, following the receipt of a request from a Responsible Supplier to do so. In the case of SMETS1 Installations comprising both a GSMS and an ESMS the Migration shall only be reattempted by the DCC where the Responsible Supplier for both Smart Metering Systems is the same.

Excluded Category – Unable to Attempt Firmware Upgrade where GroupID = "AA", "BA", or "CA"

18.9 Clause 18.2 (a) applies where:

(a) GroupID = "AA", "BA", or "CA";

(b) the SMETS1 SMS is a Dormant Meter; and

(c) the DCC has taken all reasonable steps to obtain the correct information to allow an upgrade of the firmware for the SMETS1 SMS to be attempted but the DCC has been unable to obtain such correct information (and steps to obtain such correct information may take place prior to this Clause 18 coming into effect).

Excluded Category – Firmware Upgrade / Configuration Failure where GroupID = "CB"

18.10 Clause 18.2 (b) applies where:

(a) GroupID = "CB";

(b) a SMETS1 Installation contains solely Dormant Meters; and

(c) either:

(i) the DCC has instructed the relevant SMETS1 SMSO to take the steps described in Clause
4.26 to configure the devices at least once where GroupID = "CB" (and each such instruction may take place prior to this this Clause 18 coming into effect) and each time the steps described in Clause 4.26 have been unsuccessful as the SMETS1 SMSO has been unable to successfully complete the requested configuration; or

(ii) the Meter Operator has confirmed in writing to the DCC that the firmware has failed to upgrade successfully.

Notwithstanding that Clause 18.2 (b) applies, prior to decommissioning of the Requesting Party for the GroupID (pursuant to Clause 7), the DCC shall instruct the SMETS1 SMSO to re- attempt the steps described in Clause 4.26 for a SMETS1 Installation for which Clause 18.10
(a) to (c) applies, following the receipt of a request from the Responsible Supplier to do so. In the case of SMETS1 Installations comprising both a GSMS and an ESMS the instruction shall only be actioned by the DCC where the Responsible Supplier for both Smart Metering Systems is the same. The DCC shall commence the Migration of the SMETS1 Installation should the steps required under Clause 4.26 be successfully executed.

Excluded Category – Firmware Upgrade / Configuration Failure where GroupID = "AA", "BA", or "CA"

18.11 Clause 18.2 (b) applies where:

(a) GroupID = "AA", "BA", or "CA";

(b) a SMETS1 Installation contains solely Dormant Meters;

(c) the DCC has instructed the relevant SMETS1 SMSO to take the steps described in Clause 4.26 at least three times (and each such instruction may take place prior to this this Clause 18 coming into effect); and

(d) each time the steps described in Clause 4.26 have been unsuccessful as the SMETS1 SMSO has been unable to successfully complete the requested firmware upgrade and/or configuration.

Notwithstanding that Clause 18.2 (b) applies, prior to decommissioning of the Requesting Party for the GroupID (pursuant to Clause 7), the DCC shall instruct the SMETS1 SMSO to re- attempt the steps described in Clause 4.26 for a SMETS1 Installation for which Clause 18.11
(a) to (d) applies, following the receipt of a request from the Responsible Supplier to do so. In the case of SMETS1 Installations comprising both a GSMS and an ESMS the instruction shall only be actioned by the DCC where the Responsible Supplier for both Smart Metering Systems is the same. The DCC shall commence the Migration of the SMETS1 Installation should the steps required under Clause 4.26 be successfully executed.

Excluded Category – Data Issues

18.12 Clause 18.2 (b) applies where:

(a) the SMETS1 Installation contains solely Dormant Meter(s);

(b) the DCC has taken all reasonable steps to obtain the correct information to allow Migration of the SMETS1 Installation but the DCC has been unable to obtain such correct information (and steps to obtain such correct information may take place prior to this Clause 18 coming into effect); and

(c) the DCC reasonably believes:

(i) there are no other amendments to the Code (pursuant to Clause 1.4) that would enable the Migration of that SMETS1 Installation to be attempted; and

(ii) there is not another entry to the list of SMETS1 Eligible Product Combinations that the DCC could propose which, were it to be designated or approved by the Secretary of State, would enable the Migration of that SMETS1 Installation to be attempted.

Excluded Category – Duplicate MPANs and MPRNs

18.13 Clause 18.2 (b) applies where:

(a) the SMETS1 Installation contains solely Dormant Meter(s);

(b) either the MPAN, MPRN, or both in respect of the commissioned SMETS1 Installation or the enrolled Smart Metering System (as the case may be) are recorded:

(i) in multiple SMETS1 SMSOs; or

(ii) in at least one SMETS1 SMSO and the Smart Metering Inventory;

(c) the DCC is able to verify that:

(i) in the case of a SMETS1 Installation where neither of the Smart Metering Systems of which it is comprised is an Enrolled Smart Metering System, there is another SMETS1 Installation assigned the same MPAN and/or MPRN that has communicated with another SMETS1 SMSO in the previous 35 days;

(ii) in the case of a SMETS1 Installation where there is an Enrolled Smart Metering System assigned the same MPAN as a Smart Metering System that forms part of the SMETS1 Installation, the Enrolled Smart Metering System has communicated with DCC Systems in the previous 35 days;

(iii) in the case of a SMETS1 Installation where there is an Enrolled Smart Metering System assigned the same MPRN as a Smart Metering System that forms part of the SMETS1 Installation, the Enrolled Smart Metering System has communicated with DCC Systems in the previous 35 days; or

(iv) in the case of a SMETS1 Installation where neither of the Smart Metering Systems of which it is comprised is an Enrolled Smart Metering System, the SMETS1 Installation has not communicated with the SMETS1 SMSO in the previous 35 days; and

(d) the DCC has taken all reasonable steps to obtain the correct information to allow Migration of the SMETS1 Installation to commence but the DCC has been unable to obtain such correct information (and steps to obtain such correct information may take place prior to this Clause 18 coming into effect).

Excluded Category – Dormant not due to Change of Supplier

18.14 Clause 18.2 (a) applies where, pursuant to Clause 18.2A, the Responsible Supplier for that SMETS1 Installation has provided the confirmation set out in 18.2A (d).

Excluded Category – Uneconomic to Test

18.15 Subject to Clause 18.16, Clause 18.2 (c) applies where the Secretary of State has agreed with the DCC's proposal that it is not economic to test the relevant DMC pursuant to Clause 20.7 of Appendix AK.

18.16 The Secretary of State may issue directions to the DCC to develop further proposals for amendments to the Code that would enable SMETS1 Installations excluded by Clause 18.15 to become eligible for Migration. Where such a direction is issued the proposals shall be developed in accordance with the process described in Clause 1.4.

Excluded Category – Firmware Upgrade / Configuration Failure where GroupID = "DA", "EA", or "EB"

18.17 Clause 18.2 (b) applies where:

(a) GroupID = "DA", "EA", or "EB";

(b) a SMETS1 Installation contains solely Dormant Meters;

(c) the DCC has instructed the relevant SMETS1 SMSO to take the steps described in Clause 4.26 (and such instruction may take place prior to this this Clause 18.17 coming into effect);

(d) the steps described in Clause 4.26 have been unsuccessful as the SMETS1 SMSO has been unable to successfully complete the requested firmware upgrade and/or configuration; and

(e) the DCC reasonably believe that:

(i) there is not another entry to the list of SMETS1 Eligible Product Combinations that it could propose which, were it to be approved by the Secretary of State, would enable the Migration of that SMETS1 Installation to be attempted; and

(ii) such SMETS1 Installation would be capable of successful Migration were an appropriate entry added to the list of SMETS1 Eligible Product Combinations.

Notwithstanding that Clause 18.2 (b) applies, prior to decommissioning of the Requesting Party for the GroupID (pursuant to Clause 7), the DCC shall instruct the SMETS1 SMSO to re-attempt the steps described in Clause 4.26 for a SMETS1 Installation for which Clause 18.15 (a) to (d) applies, following the receipt of a request from the Responsible Supplier to do so. In the case of SMETS1 Installations comprising both a GSMS and an ESMS the instruction shall only be actioned by the DCC where the Responsible Supplier for both Smart Metering Systems is the same. The DCC shall commence the Migration of the SMETS1 Installation should the steps required under Clause 4.26 be successfully executed.

Appendix A **Device installation – For GroupIDs "AA", "BA", "CA" and "CB"**

A1 The Application Association labels:

(a) Public

(b) Data Collection

(c) Extended Data Collection

(d) Management

(e) Firmware

shall be the names allocated by the manufacturers of Devices in this group to the Application Associations accessible to the DCC.

Installing a SMETS1 Electricity Meter

A2 The checks and processing at Table A2 shall be that required of the S1SP and DCO for 'Installing a SMETS1 Electricity Meter' for relevant GroupID and shall take place in the order specified in that Table.

Error code on failure	**S1SP checks and processing**	**DCO checks and processing**	**SupportingData**
	Should any of the following checks fail, checking and processing in relation to that SMETS1 Installation shall not proceed to a subsequent step.		
ET01	For each of the CHF, GPF (for GroupID = "AA", only where a GSMEDetail element is also present) and ESME, confirm that reading of the Public Application Association returns valid data, including all the device counters required by the subsequent steps in this table.		DeviceID
ET02	For each EncryptedMasterKey for this SMETS1 Installation, request that the DCO process the EncryptedMasterKey, and where that is successful, store the digitally signed package provided in response.	Confirm that the details provided are semantically identical to the corresponding EncryptedMasterKey in the corresponding Migration Group Encrypted File. Decrypt the EncryptedKey, re-encrypt that key with a secret key known only to the DCO, package that re-encrypted key with relevant Device IDs from the Migration Common File, then digitally sign and pass back the signed package to the S1SP .	EncryptedMasterKey
ET03	NOT USED		

Error code on failure	S1SP checks and processing	DCO checks and processing	SupportingData
ET04	Using the AuthenticationKey and EncryptionKey in each of the DataCollectionAssociation, ManagementAssociation and FirmwareAssociation within each of the CHFDetails, GPFDetails (for GroupID = "AA", only where a GSMEDetail element is also present) and ESMEDetails: 1. confirm the successful creation of an Application Association with the Device in question, 2. close each such Application Association 3. securely store each key and its association with: ○ Its 'key type' ○ the 'name of Application Association' ○ the Device ID For clarity, this is to confirm that all keys operate before any are changed.		DeviceID || 'name of Application Association' Where 'name of Application Association' is one of DataCollectionAssociation, ExtendedDataCollectionAssociation, ManagementAssociation or FirmwareAssociation
ET05	Using the AuthenticationKey and EncryptionKey in the ExtendedDataCollectionAssociation in the CHFDetails: 1. confirm the successful creation of an Application Association with the Device, 2. read the CHF Whitelist, 3. confirm the Device ID for ESME is included in CHF Whitelist where the GroupID = "AA", 4. read the serial number of the Device, 5. confirm the serial number of the Device is same as in SerialNumbers\CHF element for the SMETS1 Installation in Migration Group File 6. close the Application Association 7. securely store each key and its association with: ○ its 'key type' ○ the 'name of Application Association' ○ the Device ID ○ the serial number of the Device		1, 2, 3, 4, 5, 6 or 7 reflecting the sub step which failed
ET06	Using the AuthenticationKey and EncryptionKey in the ExtendedDataCollectionAssociation in the GPFDetails (for GroupID = "AA", only where a GSMEDetail element is also present): 1. confirm the successful creation of an Application Association with the Device, 2. NOT USED 3. close the Application Association 4. securely store each key and its association with: a. its 'key type' b. the 'name of Application Association' c. the Device ID		1, 2, 3 or 4 reflecting the sub step which failed

ET07	Using the AuthenticationKey and EncryptionKey in the ExtendedDataCollectionAssociation in the ESMEDetails: 1. confirm the successful creation of an Application Association with the Device, 2. read the serial number of the Device, 3. confirm the serial number of the Device is same as in SerialNumbers\ESME element for the SMETS1 Installation in Migration Group File 4. read the Payment Mode (with its SMETS1 meaning) 5. if the Payment Mode is prepayment (with its SMETS1 meaning), read the UTRN Meter ID form the Device. 6. then close the Application Association 7. securely store each key and its association with: a. its ‘key type’ b. the ‘name of Application Association’ c. the Device ID d. the serial number of the Device 8. If the Payment Mode is prepayment (with its SMETS1 meaning): a. for SMETS1 Installations where the GroupID = “BA”, confirm the following are present and populated validly within the ESMEDetail of the DecryptedS1SPGroupInformation for the entry with the CHFIdentifier for this SMETS1 Installation: • PrepaymentKey • WrappedPrepaymentKey b. for SMETS1 Installations where the GroupID = “CA”, confirm the following are present and populated validly within the ESMEDetail of the DecryptedS1SPGroupInformation for the entry with the CHFIdentifier for this SMETS1 Installation: • PrepaymentKey • PrepaymentWrapperKey else if the Payment Mode is Credit (with its SMETS1 meaning): a. for SMETS1 Installations where the GroupID = “CA” or “CB”, if PrepaymentWrapperKey is present and populated validly within the ESMEDetail of the DecryptedS1SPGroupInformation for the entry with the CHFIdentifier for this SMETS1 Installation, securely store the PrepaymentWrapperKey and its association to the ESME Device ID. If the Payment Mode is prepayment (with its SMETS1 meaning), using the AuthenticationKey and EncryptionKey in the ManagementAssociation in the ESMEDetails: 9. confirm the successful creation of an Application Association with the Device, 10. create and send a zero value ‘Add Credit’ instruction, 11. confirm receipt of a successful response from the Device, 12. close the Application Association, 13. securely store the PrepaymentKey, PrepaymentWrapperKey and its association to the ESME Device ID, 14. set PrepayFlag attribute as true for the SMETS1 Installation in the S1SP Commissioning File		1, 2, 3, 4, 5, 6, 7, 8, 9 ,10, 11, 12, 13 or 14 reflecting the sub step which failed

Table A2

Installing a SMETS1 GSME

A3 The processing at Table A3 shall be that required of the S1SP and DCO for 'Installing a SMETS1 GSME' for this GroupID.

Error code on failure	S1SP checks and processing	DCO checks and processing	SupportingData
	Should any of the following checks fail, checking and processing in relation to that SMETS1 Installation shall not proceed to a subsequent step		
GT01	Using the DeviceID for the CHF on which the GSME should have been whitelisted: 1. Retrieve the AuthenticationKey and EncryptionKey for the Extended Data Collection Application Association 2. Using those keys, confirm the successful creation of an Application Association with the Device, 3. read the CHF Whitelist 4. confirm that the GSME's Device ID is on that CHF Whitelist and that the GSME has communicated in the last 72 hours, 5. close the Application Association		1, 2, 3, 4, or 5 reflecting the sub step which failed

Error code on failure	S1SP checks and processing	DCO checks and processing	SupportingData
GT02	Using the Device ID of the GPF associated with the GSME 1. Retrieve the AuthenticationKey and EncryptionKey for the Extended Data Collection Application Association 2. Using those keys, confirm the successful creation of an Application Association with the Device, 3. read the serial number of the Device, 4. for SMETS1 Installations where the GroupID = “BA” only, confirm the serial number of the Device is same as in SerialNumbers\ESME element for the SMETS1 Installation in Migration Group File, 5. read the Payment Mode (with its SMETS1 meaning) 6. if the Payment Mode is prepayment (with its SMETS1 meaning), read the UTRN Meter ID form the Device. 7. then close the Application Association 8. securely store the serial number of the Device and its association to the GSME Device ID 9. If the Payment Mode is prepayment (with its SMETS1 meaning): a. for SMETS1 Installations where the GroupID = “BA”, for the GSME identified in the GSMEIdentifier for this SMETS1 Installation in the Migration Common File, confirm the following are present and populated validly within the DecryptedS1SPGroupInformation for the GSMEDetails within the entry with the CHFIdentifier for this SMETS1 Installation: • PrepaymentKey • WrappedPrepaymentKey b. for SMETS1 Installations where the GroupID = “CA” or “CB”, for the GSME identified in the GSMEIdentifier for this SMETS1 Installation in the Migration Common File, confirm the following are present and populated validly within the DecryptedS1SPGroupInformation for the GSMEDetails within the entry with the CHFIdentifier for this SMETS1 Installation: • PrepaymentKey • PrepaymentWrapperKey else if the Payment Mode is Credit (with its SMETS1 meaning): a. for SMETS1 Installations where the GroupID = “CA” or “CB”, if either of the following are present and populated validly within the GSMEDetail of the DecryptedS1SPGroupInformation for the entry with the CHFIdentifier for this SMETS1 Installation, securely store with its association to the GSME Device ID: • PrepaymentWrapperKey • WrappedPrepaymentKey If the Payment Mode is prepayment (with its SMETS1 meaning), using the AuthenticationKey and EncryptionKey in the ManagementAssociation of the GPFDetail of the GPF associated with the GSMEDetails: 10. confirm the successful creation of an Application Association with the Device, 11. create and send a zero value ‘Add Credit’ instruction, 12. confirm receipt of a successful response from the Device 13. close the Application Association 14. securely store the PrepaymentKey, PrepaymentWrapperKey and its association to the GSME Device ID 15. set PrepayFlag attribute as true for the SMETS1 Installation in S1SP Commissioning File.		1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14 or 15 reflecting the sub step which failed

Table A3

Installing a SMETS1 PPMID

A4 The processing at Table A4 shall be that required of the S1SP and DCO for ‘Installing a SMETS1 PPMID’ for this GroupID.

Error code on failure	S1SP checks and processing	DCO checks and processing	SupportingData
	Should any of the following checks fail, checking and processing in relation to that SMETS1 Installation shall not proceed to a subsequent step		
	NOT USED		

Table A4

Commission Device (CHF)

A5 The processing at Table A5 shall be that required of the S1SP and DCO for 'Commission Device (CHF)' for this GroupID.

Error code on failure	S1SP checks and processing	DCO checks and processing	SupportingData
DP01	Instruct the DCC to add the relevant CHF details to the Smart Metering Inventory.		

Table A5

Securing a SMETS1 ESME

A6 The checks and processing at Table A6 shall be that required of the S1SP and DCO for 'Securing a SMETS1 ESME' for relevant GroupID and shall take place in the order specified in that Table.

Error code on failure	S1SP checks and processing	DCO checks and processing	SupportingData
	Should any of the following checks fail, checking and processing in relation to that SMETS1 Installation shall not proceed to a subsequent step		
ET08	For each EncryptedMasterKey for this SMETS1 Installation that relates to an ESME and / or CHF and / or (where a GSMEDetail element is also present) GPF: 1. Generate a new value for the EncryptionKey for the DataCollectionAssociation for one of the Devices within EncryptedMasterKey 2. Request that the DCO creates, using the relevant Master Key, the relevant form of the EncryptionKey for inclusion in key change instructions to the Device 3. Request that the Device changes to use the new key in this Application Association 4. Confirm that the Device has switched to using the new key 5. securely store the new key and its association with: o its 'key type' o the 'name of Application Association' o the Device ID 6. invalidate the replaced key	Create the relevant form of key required for inclusion in the instructions using the relevant Master Key.	DeviceID, so identifying the Master Key which is not functioning

Table A6

Appendix B Device Installation – For GroupID = "EA" or "EB"

B1 The Application Association labels:

(a) Application Association G

shall be the names allocated by the manufacturers of the SMETS1 ESMEs in this group to the Application Associations accessible to the DCC.

Installing a SMETS1 Electricity Meter

B2 The checks and processing at Table B2 shall be that required of the S1SP and DCO for 'Installing a SMETS1 Electricity Meter' and shall take place in the order specified in that Table.

Error code on failure	S1SP checks and processing	SupportingData
	Should any of the following checks fail, checking and processing in relation to that SMETS1 Installation shall not proceed to a subsequent step.	
ET01	Using the DeviceCertificate in the CHFDetails\DeviceCertificate element which the ESME is associated with, 1) initialise network connection with CHF confirming successful responses to messages 2) confirm the successful creation of a TLS session with the CHF in question. 3) read the CHF Whitelist, 4) confirm the Device ID in the Migration Common File for the ESME is included in the CHF Whitelist,	1, 2, 3, 4 reflecting the sub step which failed
ET02	Using the Device ID for the ESME, 1. confirm the successful creation of an Application Association G with the Device 2. Not Used 3. Not Used 4. read the Payment Mode (with its SMETS1 meaning) of the Device, if the Payment Mode is prepayment (with its SMETS1 meaning): a. confirm the following are present and populated validly within the ESMEDetail of the DecryptedS1SPDPGroupInformation for the entry with the CHFIdentifier for this SMETS1 Installation: i. PrepaymentKey 5. close the Application Association G 6. if the payment mode is Prepayment Mode (with its SMETS1 meaning), set the PrepayFlag attribute as true for the SMETS1 Installation in the S1SP Commissioning File 7. securely store the PrePaymentKey and its association with: a. its 'key type' b. the Device ID	1, 2, 3, 4, 5, 6 or 7 reflecting the sub step which failed
ET03	Using the AuthenticationKey and EncryptionKey within the ESMEDetails: 1. confirm the successful creation of an Application Association G using High Level Security (with its DLMS meaning) with target ESME, 2. close the Application Association G using High Level Security (with its DLMS meaning) 3. securely store AuthenticationKey and EncryptionKey in addition to their association with: ○ its 'key type' ○ the 'name of Application Association' ○ the Device ID For clarity, this is to confirm that all keys operate before any are changed.	1, 2 or 3 reflecting the sub step which failed

Table B2

Installing a SMETS1 GSME

B3 The processing at Table B3 shall be that required of the S1SP for 'Installing a SMETS1 GSME' and shall take place in the order specified in that Table.

Error code on failure	S1SP checks and processing	SupportingData
	Should any of the following checks fail, checking and processing in relation to that SMETS1 Installation shall not proceed to a subsequent step	

Error code on failure	S1SP checks and processing	SupportingData
GT01	Using the DeviceCertificate in the CHFDetails\DeviceCertificate element which the GSME is associated with, 1. initialise network connection with CHF confirming successful responses to messages 2. confirm the successful creation of a TLS session with the CHF in question, 3. read the CHF Whitelist, 4. confirm the Device ID in the Migration Common File for the GSME is included in CHF Whitelist,	1, 2, 3 or 4 reflecting the sub step which failed
GT02	Using the Device ID of the GPF associated with the GSME 1. initialise network connection with CHF confirming successful responses to messages 2. confirm the successful creation of a TLS session with the CHF in question 3. Not Used 4. Not Used 5. read the Payment Mode (with its SMETS1 meaning) if the Payment Mode is prepayment (with its SMETS1 meaning): a. confirm that the following are present and populated validly within the GSMEDetail of the DecryptedS1SPDPGroupInformation for the entry with the CHFIdentifier of this SMETS1 installation:PrepaymentKey 6. close TLS session 7. if the Mode is prepayment (with its SMETS1 meaning), set PrepayFlag attribute as true for the SMETS1 Installation in the S1SP Commissioning File. 8. securely store PrepaymentKey and its association with: a. its 'key type' b. the Device ID	1, 2, 3, 4, 5, 6, 7 or 8 reflecting the sub step which failed

Table B3

Installing a SMETS1 PPMID

B4 No additional checks or processing is required.

Commission Device (CHF)

B5 The processing at Table B5 shall be that required of the S1SP for 'Commission Device (CHF)'.

Error code on failure	S1SP checks and processing	DCO checks and processing	SupportingData
DP01	Instruct the DCC to add the relevant CHF details to the Smart Metering Inventory.	None required	

Table B5

Securing a SMETS1 ESME

B6 The checks and processing at Table B6 shall be that required of the S1SP and DCO for 'Securing a SMETS1 ESME' for relevant GroupIDs and shall take place in the order specified in that Table.

Error code on failure	S1SP checks and processing	DCO checks and processing	SupportingData
	Should any of the following checks fail, checking and processing in relation to that SMETS1 Installation shall not proceed to a subsequent step, except where otherwise stated		

Error code on failure	S1SP checks and processing	DCO checks and processing	SupportingData
ET04	The S1SP shall connect through Application Association G using High Level Security (with its DLMS meaning), using the appropriate EncryptionKey and AuthenticationKey 1. configure the amount the clock can be adjusted daily without authorisation of the DCO to 9 seconds 2. configure security access attributes to restrict write access without authorisation of the DCO for Application Association G not using High Level Security (with its DLMS meaning) 3. verify write access changes to Application Association G not using High Level Security (with its DLMS meaning) by reading security access attribute 4. configure firmware key to prevent activation of firmware images without authorisation of the DCO		1, 2, 3 or 4 reflecting the sub step which failed
ET05	For the EncryptedMasterKey for this SMETS1 Installation that relates to an ESME, request that the DCO creates a new Master Key for the Application Association G using High Level Security (with its DLMS meaning) for inclusion in key change instruction to the Device.	DCO to check that the DeviceID is in a DCO viable installation. Create the relevant form of key required for inclusion in the instructions using the relevant Master Key.	DeviceID, so identifying the Master Key which is not functioning
ET06	Send the authorising request that the Device performs a key rotation to use the new Master Key in Application Association G using High Level Security (with its DLMS meaning).	None required	
ET07	If a response is received from the ESME indicating a successful rotation: 1. securely store the encrypted MasterKey and its association with: ○ its 'key type' ○ the 'name of Application Association' ○ the Device ID 2. invalidate the replaced key	None required	1 or 2 reflecting the sub step which failed
ET08	For the Master Key created in ET05, request the DCO creates a new EncryptionKey and AuthenticationKey for inclusion in key change instructions to the device.	Create the relevant form of key required for inclusion in the instructions using the relevant Master Key.	DeviceID, so identifying the Master Key which is not functioning
ET09	Send the authorising request that the Device performing a key rotation to use the new EncryptionKey and AuthenticationKey in Application Association G using High Level Security (with its DLMS meaning)	None required	
ET10	If a response is received from the ESME indicating a successful rotation: 1. confirm that the ESME has switched to using the new keys from the old keys 2. securely store the new encrypted Encryptionkey and AuthenticationKey along with their association with: ○ its 'key type' ○ the 'name of Application Association' ○ the Device ID 3. invalidate the replaced keys	None required	1, 2 or 3 reflecting the sub step which failed

Table B6

Configure Pushing of Profile Data

B7 The processing at Table B7 shall be that required of the S1SP for 'Configure Pushing of Profile Data' and shall take place in the order specified in that Table.

Error code on failure	S1SP checks and processing	SupportingData
	Should any of the following checks fail, checking and processing in relation to that SMETS1 Installation shall not proceed to a subsequent step, except where otherwise stated	
ET11	Attempt to configure the CHF to disable pushing of ESMS's Profile Data Log (with its SMETS1 meaning) and confirm receipt of a successful response	
GT03	Where a GSMEDetail element is present, attempt to configure the CHF to disable pushing of GSMS's Profile Data Log (with its SMETS1 meaning) and confirm receipt of a successful response	

Table B7

Appendix C Device Installation – For GroupID "DA"

Installing a SMETS1 Electricity Meter

C1 The checks and processing at Table C1 shall be that required of the DCC for 'Installing a SMETS1 Electricity Meter' and shall take place in the order specified in that Table.

Error code on failure	DCC checks and processing	SupportingData
	Should any of the following checks fail, checking and processing in relation to that SMETS1 Installation shall not proceed to a subsequent step.	
ET01	Using the DeviceID for the ESME: 1. read the Payment Mode (with its SMETS1 meaning); and 2. ensure the VendPriceChangeHANLimit is set to zero. If the Payment Mode is prepayment (with its SMETS1 meaning): 3. create and send a zero value 'Add Credit' instruction, 4. confirm receipt of a successful response from the Device, 5. store the PrepayFlag attribute as true for the SMETS1 Installation for the S1SP Commissioning File generation.	1, 2, 3, 4 or 5 reflecting the sub step which failed

Table C1

Installing a SMETS1 GSME

C2 The processing at Table C2 shall be that required of the DCC for 'Installing a SMETS1 GSME' and shall take place in the order specified in that Table.

Error code on failure	DCC checks and processing	SupportingData
	Should any of the following checks fail, checking and processing in relation to that SMETS1 Installation shall not proceed to a subsequent step	
GT01	Using the DeviceID for the CHF on which the GSME should have been whitelisted: 1. read the CHF Whitelist and 2. confirm that the GSME's Device ID is on that CHF Whitelist and that the GSME has communicated in the last 24 hours.	
GT02	Using the Device ID of the GPF associated with the GSME 1. read the Payment Mode (with its SMETS1 meaning) 2. ensure the VendPriceChangeHANLimit is set to zero. If the Payment Mode is prepayment (with its SMETS1 meaning): 3. create and send a zero value 'Add Credit' instruction, 4. confirm receipt of a successful response from the Device 5. store the PrepayFlag attribute as true for the SMETS1 Installation for the S1SP Commissioning File generation.	1, 2, 3, 4, or 5 reflecting the sub step which failed

Table C2

Installing a SMETS1 PPMID

C3 No additional checks or processing is required.

Commission Device (CHF)

C4 The processing at Table C4 shall be that required of the S1SP for 'Commission Device (CHF)'.

Error code on failure	S1SP checks and processing	DCO checks and processing	SupportingData
DP01	Instruct the DCC to add the relevant CHF details to the Smart Metering Inventory.	None required	

Table C4

Securing a SMETS1 GSME

C5 The checks and processing at Table C5 shall be that required of the S1SP and DCO for 'Securing a SMETS1 GSME' for the relevant GroupID and shall take place in the order specified in that Table.

Error code on failure	S1SP checks and processing	DCO checks and processing	SupportingData
	Should any of the following checks fail, checking and processing in relation to that SMETS1 Installation shall not proceed to a subsequent step, except where otherwise stated.		
GT03	The S1SP shall request using the GSME serial number that the DCO creates a Single Use Authorisation Code for SUAKeyDetails for the Device type GSME to bring the GSME within DCO control.	The DCO validates that serial number is currently in a DCO Viable Installation, and if so creates an authorisation instruction, containing a DCO Public Key, using the decrypted EncryptedSUAKey element, and then persists relevant information about the SMETS1 Installation.	
GT04	The S1SP shall send the authorising instruction to the GSME requesting that it performs a key rotation to come under the DCO control.	None required	
GT05	If the S1SP receives a response from the GSME indicating a success of the authorising instruction from the DCO pursuant to GT04, then the S1SP shall store: 1. the DCO Public Key; and 2. the GSME's Public Key generated as a result of this instruction and the associated Digital Signature created using the GSME's permanent Private Key.	None required	1 or 2 reflecting the sub step which failed

Error code on failure	S1SP checks and processing	DCO checks and processing	SupportingData
GT06	If the S1SP receives a response from the GSME indicating a failure of the authorising instruction from the DCO, the S1SP shall: 1. read the GSME's Public Key and the associated Digital Signature from the GSME; 2. request using the GSME serial number, the GSME's Public Key and the DCO Public Key that the DCO creates an authorising instruction to rotate the key used to authenticate instructions to the GSME; 3. sends the authorising instruction to the GSME requesting that it performs a key rotation to change the key used to authenticate instructions from the DCO.	The DCO validates the Digital Signature on the GSME public key against the Public Key stored from the installation. The DCO creates an authorisation instruction, containing a DCO Public Key, using the key derived from the GSME's Public Key and the Private Key corresponding to the supplied DCO Public Key.	1, 2 or 3 reflecting the sub step which failed
GT07	If the S1SP receives a response from the GSME indicating a success of the authorising instruction from the DCO pursuant to GT04, then the S1SP shall store: 1. the DCO Public Key; and 2. the GSME's Public Key generated as a result of this instruction and the associated Digital Signature created using the GSME's permanent Private Key.	None required	1 or 2 reflecting the sub step which failed

Table C5

Securing a SMETS1 ESME

C6 The checks and processing at Table C6 shall be that required of the S1SP and DCO for 'Securing a SMETS1 ESME' for the relevant GroupID and shall take place in the order specified in that Table.

Error code on failure	S1SP checks and processing	DCO checks and processing	SupportingData
	Should any of the following checks fail, checking and processing in relation to that SMETS1 Installation shall not proceed to a subsequent step, except where otherwise stated		
ET03	The S1SP shall request using the ESME serial number that the DCO creates a Single Use Authorisation Code for SUAKeyDetails for the Device type ESME to bring the ESME within DCO control.	The DCO validates that serial number is currently in a DCO Viable Installation, and if so creates an authorisation instruction, containing a DCO Public Key, using the decrypted EncryptedSUAKey element, and then persists relevant information about the SMETS1 Installation.	

Error code on failure	S1SP checks and processing	DCO checks and processing	SupportingData
ET04	The S1SP shall send the authorising instruction to the ESME requesting that it performs a key rotation to come under the DCO control.	None required	
ET05	If the S1SP receives a response from the ESME indicating a success of the authorising instruction from the DCO pursuant to ET04, then the S1SP shall store: 1. the DCO Public Key; and 2. the ESME's Public Key generated as a result of this instruction and the associated Digital Signature created using the ESME's permanent Private Key.	None required	1 or 2 reflecting the sub step which failed
ET06	If the S1SP receives a response from the ESME indicating a failure of the authorising instruction from the DCO, the S1SP shall: • read the ESME's Public Key and the associated Digital Signature from the ESME; • request using the ESME serial number, the ESME's Public Key and the DCO Public Key that the DCO creates an authorising instruction to rotate the key used to authenticate instructions to the ESME; • sends the authorising instruction to the ESME requesting that it performs a key rotation to change the key used to authenticate instructions from the DCO.	The DCO validates the Digital Signature on the ESME public key against the Public Key stored from the installation. The DCO creates an authorisation instruction, containing a DCO Public Key, using the key derived from the ESME's Public Key and the Private Key corresponding to the supplied DCO Public Key.	1, 2 or 3 reflecting the sub step which failed
ET07	If the S1SP receives a response from the ESME indicating a success of the authorising instruction from the DCO pursuant to ET03, then the S1SP shall store: 1. the DCO Public Key; and 2. the ESME's Public Key generated as a result of this instruction and the associated Digital Signature created using the ESME's permanent Private Key.	None required	1 or 2 reflecting the sub step which failed

Table C6

Version AM 13.0

APPENDIX AM

SMETS1 Supporting Requirements

1 Introduction

1.1 This document lays out supporting requirements in relation to SMETS1 Devices and communications relating to SMETS1 Devices. None of the provisions in this document apply to SMETS2+ Devices nor to communications relating to them.

2 Defined Terms

Term	Meaning
||	X || Y shall mean the concatenation of the two octet strings X and Y.
Alert Code	For a SMETS1 Alert, shall mean the value placed in the GBCSHexAlertCode field (with its Message Mapping Catalogue meaning).
Authorising Remote Party Signature	Shall have the meaning specified in Clause 16.1.
Category 1 Device	Shall mean for the purposes of Section G2.44A of this Code, all SMETS1 Devices for which the "Group ID" for that Device Model in the SMETS1 Eligible Product Combinations List is 'DA'.
Category 2 Device	Shall mean for the purposes of Section G2.44A of this Code any SMETS1 Device that is not a Category 1 Device.
Certificate ID	In relation to an Organisation Certificate, shall be the combination of `serialNumber` and Issuer X520 Common Name (each with their Organisation Certificate Policy meanings) and so shall be a unique identifier for that Certificate.
Critical Instruction	Shall mean an Instruction that has the potential to affect the supply of energy to the premises or the security of any Device installed in the premises (but excluding any Instruction that is expected to increase the amount of credit available to the consumer).
SMETS1 CHF Device Log	Shall have the meaning specified in Clause 17.49.
CoS Execution Counter	Shall have the meaning specified in Clause 11.2(a).

Term	**Meaning**
Device Security Credentials	In relation to a SMETS1 Device, Device Security Credentials shall include the Certificates identified by Notified Critical Supplier Certificate ID, Notified Non-Critical Supplier Certificate ID, Notified Critical Network Operator Certificate ID and Notified Non-Critical Network Operator Certificate ID.
Event Code	For a SMETS1 Response containing Security Log or Event Log entries (with their SMETS1 meanings), shall mean the SMETS1 Mandated Event Code or the SMETS1 Non-Mandated Event Code in an entry.
Event/Alert Code	Shall mean the Alert Code or the Event Code, as required by the context.
Execution Counter	Shall have the meaning specified in Clause 11.1(a).
IEEE	The Institute of Electrical and Electronics Engineers.
Message Code	For a SMETS1 Alert, shall mean the SMETS1 Mandated Event Message Code or the SMETS1 Non-Mandated Event Message Code. For a SMETS1 Response, shall mean the value of GBCSHexadecimalMessageCode (with its Message Mapping Catalogue meaning) required by Clause 9.
Most Recently Verified Manufacturer Image Hash	Shall have the meaning laid out at Clause 16.5 (as updated in accordance with Clause 17.57).
Notified Critical Network Operator Certificate ID	Shall be the Certificate ID most recently recorded by the relevant S1SP in relation to a SMETS1 Device pursuant to Clause 18, with the Certificate ID having the values from the Certificate in the Service Request where Remote Party Role is 'networkOperator' and keyUsage is '`digitalSignature`' (all with their Organisation Certificate Policy meanings).
Notified Critical Network Operator ID	Shall be the Entity Identifier (with its Organisation Certificate Policy meaning) most recently recorded by the relevant S1SP in relation to a SMETS1 Device pursuant to Clause 18, with the Entity Identifier having the value from the Certificate in the Service Request where Remote Party Role is 'networkOperator' and keyUsage is '`digitalSignature`' (all with their Organisation Certificate Policy meanings).

Term	**Meaning**
Notified Critical Supplier Certificate ID	Shall be the Certificate ID most recently recorded by the relevant S1SP in relation to a SMETS1 Device pursuant to Clause 18, with the Certificate ID having the values from the Certificate in the Service Request where Remote Party Role is 'supplier' (with its Section L meaning) and `keyUsage` is '`digitalSignature`'(each with their Organisation Certificate Policy meanings).
Notified Critical Supplier ID	Shall be the Entity Identifier (with its Organisation Certificate Policy meaning) most recently recorded by the relevant S1SP in relation to a SMETS1 Device pursuant to Clause 18, with the Entity Identifier having the value from the Certificate in the Service Request where Remote Party Role is 'supplier' and keyUsage is '`digitalSignature`' (all with their Organisation Certificate Policy meanings).
Notified Non-Critical Network Operator Certificate ID	Shall be the Certificate ID most recently recorded by the relevant S1SP in relation to a SMETS1 Device pursuant to Clause 18, with the Certificate ID having the values from the Certificate in the Service Request where Remote Party Role is 'networkOperator' and keyUsage is '`keyAgreement`' (all with their Organisation Certificate Policy meanings).
Notified Non-Critical Supplier Certificate ID	Shall be the Certificate ID most recently recorded by the relevant S1SP in relation to a SMETS1 Device pursuant to Clause 18, with the Certificate ID having the values from the Certificate in the Service Request in the KeyAgreementCertificate data item, where the RemotePartyRole data item has the value of Supplier (each with their DUIS meanings).
Notified Non-Critical Supplier ID	Shall be the Entity Identifier (with its Organisation Certificate Policy meaning) most recently recorded by the relevant S1SP in relation to a SMETS1 Device pursuant to Clause 18, with the Entity Identifier having the value from the Certificate in the Service Request in the KeyAgreementCertificate data item where the RemotePartyRole data item has the value of Supplier (with their DUIS meanings).
Notified Non-Critical Network Operator ID	Shall be the Entity Identifier (with its Organisation Certificate Policy meaning) most recently recorded by the relevant S1SP in relation to a SMETS1 Device pursuant to Clause 18, with the Entity Identifier having the value from the Certificate in the Service Request where Remote Party Role is 'networkOperator' and keyUsage is '`keyAgreement`' (all with their Organisation Certificate Policy meanings).
Originator Counter	Shall have the meaning laid out at Clause 5.
OTA Header	Shall have the meaning laid out at Clause 16.3.

Term	Meaning
OTA Upgrade Image	Shall have the meaning laid out at Clause 16.4.
S1SP Time	In relation to an S1SP, shall be the time measured by a time source used by that S1SP pursuant to Clause 10.
SMETS1 Mandated Event	Shall have the meaning laid out at Clause 8.1.
SMETS1 Mandated Event Code	In a SMETS1 Alert or a Countersigned SMETS1 Alert, shall be the value placed in the GBCSHexAlertCode field (with its Message Mapping Catalogue meaning) as required by Clause 8.7(b).
SMETS1 Mandated Event Message Code	In a SMETS1 Alert or a Countersigned SMETS1 Alert created as a result of a SMETS1 Mandated Event, shall be the value placed in the GBCSHexadecimalMessageCode field (with its Message Mapping Catalogue meaning) as required by Clause 8.5.
SMETS1 Message Code	In a SMETS1 Response or a Countersigned SMETS1 Response, shall be the value placed in the GBCSHexadecimalMessageCode field (with its Message Mapping Catalogue meaning) as required by Clause 9.1. In a SMETS1 Alert or a Countersigned SMETS1 Alert, shall be either the SMETS1 Mandated Event Message Code or the SMETS1 Non-Mandated Event Message Code, as determined by Clauses 8.5 and 8.7(a).
SMETS1 Non-Mandated Event	Shall have the meaning laid out at Clause 8.3.
SMETS1 Non-Mandated Event Code	Shall have the meaning laid out at Clause 8.3(a).
SMETS1 Non-Mandated Event Description	Shall have the meaning laid out at Clause 8.3(b).
SMETS1 Non-Mandated Event Message Code	In a SMETS1 Alert or a Countersigned SMETS1 Alert created as a result of a SMETS1 Non-Mandated Event, shall be the hexBinary value of 1000 (where hexBinary has the meaning defined at http://www.w3.org/TR/xmlschema-2/#hexBinary) placed in the GBCSHexadecimalMessageCode field (with its Message Mapping Catalogue meaning).
Time-based Debt Recovery	Shall have the meaning set out in SMETS1.

Term	Meaning
Unknown Remote Party (URP)	In relation to a SMETS1 Device, shall mean a Party for which the relevant S1SP does not hold either a current Notified Critical Supplier ID or a current Notified Critical Network Operator ID for the SMETS1 Device in question.
Unsupported Value	Shall have the meaning set out in DUIS.
Upgrade Image	Shall have the meaning laid out at Clause 16.2.

2.1 Additionally, where defined terms from specific parts of the Code are used, the relevant part of the Code is stated. Where no part of the Code is stated, a defined term shall have its Section A meaning.

3 Device IDs

3.1 A Party notifying a SMETS1 Device's details to the DCC for recording in the Smart Metering Inventory shall notify the Device's Device ID according to the requirements of Table 1.

Type of SMETS1 Device	Requirement for Device ID
SMETS1 CHF	The Device ID shall be an identifier that the notifying Party has ensured is EUI-64 Compliant.
SMETS1 ESME	Where the Device's only network interface is one complying with ZigBee Alliance standards, the Device ID shall be the IEEE address associated with that network interface. Otherwise, the Device ID shall be an identifier that the notifying Party has ensured is EUI-64 Compliant.
SMETS1 GSME, SMETS1 GPF, SMETS1 PPMID, SMETS1 IHD or	The Device ID shall be the IEEE address associated with the Device's network interface which implements ZigBee Alliance standards.

any other device operating on a home area network created by a SMETS1 CHF	

Table 1

4 User IDs in Service Requests

4.1 In relation to 'Top Up Device' (SRV 2.2) and all Critical Service Requests where the Device Type of the target Device is neither 'CHF' nor ‘PPMID’, a User shall use its Notified Critical Supplier ID or its Notified Critical Network Operator ID (as the context requires) for the Device whose Device ID is in the BusinessTargetID field (with its DUIS meaning) in the Service Request and shall create a Digital Signature within which the Certificate ID identifies a Certificate with an Entity Identifier having the same value as its Notified Critical Supplier ID or its Notified Critical Network Operator ID (as the context requires). In relation to Critical Service Requests where the Device Type of the target Device is 'CHF' or ‘PPMID’ (specifically 'Activate Firmware' (SRV 11.3)), a User shall use its Notified Critical Supplier ID for the ESME that is on the same home area network as the CHF or PPMID (as the context requires) whose Device ID is in the BusinessTargetID field (with its DUIS meaning) in the Service Request and shall create a Digital Signature within which the Certificate ID identifies a Certificate with an Entity Identifier having the same value as its Notified Critical Supplier ID. In relation to all other Service Requests, a User may use any User ID which the DCC has previously accepted in relation to the User acting in the User Role in which the User wishes to have the Service Request in question processed by the DCC.

4.2 On receipt of a 'Top Up Device' or Critical Service Request, the S1SP shall confirm that the target Device's Notified Critical Supplier ID or Notified Critical Network Operator ID (as the context requires), or where the target Device's Device Type is 'CHF' or ‘PPMID’, the Notified Critical Supplier ID of the ESME on the same home area network, is that specified in the BusinessOriginatorID field (with its DUIS meaning) in the Service Request and is the Entity Identifier within the Certificate used to Check Cryptographic Protection on the Service Request and where it is not, the S1SP shall create and send a SMETS1 Response notifying failure and shall undertake no further processing.

5 Originator Counters

5.1 Except for ‘Update Security Credentials (CoS) (SRV 6.23)’ SMETS1 Service Requests, in relation to each SMETS1 Service Request that a User creates using a specific User ID and a specific Device ID, the User shall ensure that the Originator Counter is a 64-bit unsigned integer that is numerically greater than both zero and the value it has used in relation to any previous Service Request containing the same User ID and Device ID.

5.2 In relation to each 'Update Security Credentials (CoS) (SRV 6.23)' SMETS1 Service Request that a User creates, the User shall ensure that the Originator Counter is a 64-bit unsigned integer that is numerically greater than the value it has used in relation to any previously created 'Update Security Credentials (CoS) (SRV 6.23)' SMETS1 Service Request.

5.3 In relation to each SMETS1 Alert created using a specific Device ID and a specific User ID, the S1SP shall ensure that the Originator Counter is a 64-bit unsigned integer that is numerically greater than the value it has used in relation to any previous SMETS1 Alert containing the same User ID and Device ID.

6 Related Identifiers & Counters

6.1 In relation to any SMETS1 Service Request targeted at a SMETS1 Device, the sending User shall, within the RequestID field (with its DUIS meaning), populate:

(a) BusinessOriginatorID (with its DUIS meaning) with a User ID complying with Clause 4;

(b) BusinessTargetID (with its DUIS meaning) with the Device's Device ID, where that Device ID complies with Clause 3; and

(c) OriginatorCounter (with its DUIS meaning) with an Originator Counter complying with Clause 5.1 or Clause 5.2 (as relevant).

6.2 In relation to any SMETS1 Response, any Countersigned SMETS1 Response, any S1SP Alert and any Countersigned S1SP Alert, the DCC and the S1SP shall:

(a) populate any RequestID field (with its DUIS meaning) with the value of the RequestID in the corresponding SMETS1 Service Request;

(b) within any ResponseID field (with its DUIS meaning) and within the fields themselves, populate:

(i) any BusinessOriginatorID field (with its DUIS and Message Mapping Catalogue meaning) with the value of the BusinessTargetID in the

RequestID as identified in Clause 6.1(b);

(ii) any BusinessTargetID field (with its DUIS and Message Mapping Catalogue meaning) with the value of the BusinessOriginatorID in the RequestID as identified in Clause 6.1(a); and

(iii) any OriginatorCounter field (with its DUIS and Message Mapping Catalogue meaning) with the value of the OriginatorCounter in the RequestID as identified in Clause 6.1(c).

6.3 In relation to any SMETS1 Alert, the S1SP shall populate:

(a) any BusinessOriginatorID field (with its DUIS and Message Mapping Catalogue meaning) with the Device's Device ID, where that Device ID complies with Clause 3;

(b) any BusinessTargetID field (with its DUIS and Message Mapping Catalogue meaning) in accordance with Clause 8.6 and 8.7; and

(c) any OriginatorCounter field (with its DUIS and Message Mapping Catalogue meaning) with an Originator Counter complying with Clause 5.3.

7 <u>Supplementary Party Details</u>

7.1 Where, in processing a SMETS1 Service Request, the DCC would have included a Supplementary Remote Party ID value and a Supplementary Remote Party Counter value (with their GBCS meanings) in a resulting Command if the target Device had been a SMETS2+ Device, the DCC shall include those values in the Countersigned Service Request sent to the relevant S1SP, and shall identify those details as being a Supplementary Remote Party ID value and a Supplementary Remote Party Counter value respectively (with their GBCS meanings).

7.2 Where an S1SP creates a SMETS1 Response where the corresponding Countersigned Service Request contained details identified as a Supplementary Remote Party ID value and a Supplementary Remote Party Counter value, the S1SP shall use those values to populate the SupplementaryRemotePartyID and SupplementaryRemotePartyCounter fields (with their Message Mapping Catalogue meaning). For clarity, the S1SP shall not incorporate a SupplementaryOriginatorCounter field (with its Message Mapping Catalogue meaning) in any SMETS1 Response.

8 Event logging and alerts

8.1 SMETS1 requires that a number of events can be detected by SMETS1 Devices and that an occurrence of such an event triggers:

(a) the sending of an alert over a WAN interface (with its SMETS1 meaning); or

(b) the recording of the event in either the Event Log or the Security Log (with their SMETS1 meanings); or

(c) both the sending of such an alert over a WAN interface and the recording of the event in either the Event Log or the Security Log (with their SMETS1 meanings).

8.2 Table 2 identifies the SMETS1 requirements for Devices to detect events and the associated alerting and logging requirements. Additionally, the Service Request Processing Document (SRPD) requires that when processing a SMETS1 'Update Firmware' (SRV11.1) Service Request, the S1SP undertakes verification of the FirmwareImage (with its DUIS meaning). This can lead to one of two events: (1) the verification succeeds or (2) the verification fails. Both events are also included in Table 2. Events (described in the column headed "AlertDescription / LogMeaning) in Table 2 are referred to as "SMETS1 Mandated Events" in this document.

Specification of the SMETS1 Mandated Event	GBCSHexadecimal MessageCode	GBCSHexAlertCode / LogCode	AlertDescription / LogMeaning	BusinessTargetID	SMETS1 Alert required?	Logging Required? (No / Event Log / Security Log)
SMETS1 5.3.5.1 (ii) / (iii)	1000	8F01	Active Power Import above Load Limit Threshold	Notified Critical Supplier ID	Yes	Event Log
SMETS1 5.3.10.1 (ii) (a) / (c)	1001	8F40	SMETS1 Average RMS Voltage above Average RMS Over Voltage Threshold	Notified Non-Critical Network Operator ID	Yes	Event Log
SMETS1 5.3.10.1 (iii) (a) / (c)	1001	8F41	SMETS1 Average RMS Voltage below Average RMS Under Voltage Threshold	Notified Non-Critical Network Operator ID	Yes	Event Log
SMETS1 4.3.6.2 (iv) SMETS1 5.3.6.2 (iv)	1001	810D	Combined Credit Below Low Credit Threshold (prepayment mode)	Notified Non-Critical Supplier ID	Yes	No
SMETS1 4.3.6.2 (v) SMETS1 5.3.6.2 (v)	1000	8F0F	Credit Below Disablement Threshold (prepayment mode)	Notified Critical Supplier ID	Yes	No
SMETS1 4.3.5.2 (v)	1000	8F1D	GSME Power Supply Loss	Notified Critical Supplier ID	Yes	No

Specification of the SMETS1 Mandated Event	GBCSHexadecimal MessageCode	GBCSHexAlertCode / LogCode	AlertDescription / LogMeaning	BusinessTargetID	SMETS1 Alert required?	Logging Required? (No / Event Log / Security Log)
SMETS1 4.3.5.1 (i)/(ii)	1000	8F1F	Low Battery Capacity	Notified Critical Supplier ID	Yes	Event Log
SMETS1 4.4.2.2 SMETS1 4.4.3.2 SMETS1 4.4.3.4 SMETS1 5.4.3.2 SMETS1 5.4.4.2 SMETS1 5.5.4.4	1000	8F32	Supply Armed	Notified Critical Supplier ID	Yes	No
SMETS1 5.3.5.1 (v)	1000	8F33	Supply Disabled then Armed - Load Limit triggered	Notified Critical Supplier ID	Yes	No
SMETS1 5.3.10.2 (i) / (ii)	1001	8020	RMS Voltage above Extreme Over Voltage Threshold (voltage rises above for longer than the configurable period)	Notified Non-Critical Network Operator ID	Yes	Event Log
SMETS1 5.3.10.5 (i) / (ii)	1001	8024	RMS Voltage above Voltage Swell Threshold (voltage rises above for longer than the configurable period)	Notified Non-Critical Network Operator ID	Yes	Event Log
SMETS1 5.3.10.3 (i) / (ii)	1001	8028	RMS Voltage below Extreme Under Voltage Threshold (voltage falls below for longer than the configurable period)	Notified Non-Critical Network Operator ID	Yes	Event Log
SMETS1 5.3.10.4 (i) / (ii)	1001	802C	RMS Voltage below Voltage Sag Threshold (voltage falls below for longer than the configurable period)	Notified Non-Critical Network Operator ID	Yes	Event Log
SMETS1 4.3.9.3 (viii) / (viii) SMETS1 5.3.9.3 (viii) / (viii)	1000	8F3E	Unauthorised Communication Access attempted	Notified Critical Supplier ID	Yes	Security Log
SMETS1 4.3.9.2 (viii) / (ix) SMETS1 5.3.9.2 (viii) / (ix)	1000	8F3F	Unauthorised Physical Access - Tamper Detect	Notified Critical Supplier ID	Yes	Security Log
SRPD 16.1	00CE	8F1C	Firmware Verification Failed (ESME)	Notified Critical Supplier ID	Yes	No
SRPD 16.1	00CE	8F72	Firmware Verification Successful (ESME)	Notified Critical Supplier ID	Yes	No
SRPD 16.1	00CF	8F1C	Firmware Verification Failed (GSME)	Notified Critical Supplier ID	Yes	No
SRPD 16.1	00CF	8F72	Firmware Verification Successful(GSME)	Notified Critical Supplier ID	Yes	No
SRPD 16.1	1002	8F1C	Firmware Verification Failed (CH)	Notified Critical Supplier ID for the ESME on the same home area network	Yes	No
SRPD 16.1	1003	8F72	Firmware Verification Successful (CH)	Notified Critical Supplier ID for the ESME on the same home area network	Yes	No
SRPD 16.1	1002	8F1C	Firmware Verification Failed (PPMID)	Notified Critical Supplier ID for the ESME on the same home area network	Yes	No

Specification of the SMETS1 Mandated Event	GBCSHexadecimal MessageCode	GBCSHexAlertCode / LogCode	AlertDescription / LogMeaning	BusinessTargetID	SMETS1 Alert required?	Logging Required? (No / Event Log / Security Log)
SRPD 16.1	1003	8F72	Firmware Verification Successful (PPMID)	Notified Critical Supplier ID for the ESME on the same home area network	Yes	No
SMETS1 4.3.2 SMETS1 5.3.2	N/A	8F3D	Trusted Source Authentication Failure	N/A	No	Security Log
SMETS1 4.3.9.1 SMETS1 5.3.9.1	N/A	8F53	Failed Authentication or Authorisation not covered by other codes	N/A	No	Security Log
SMETS1 4.3.9.1 SMETS1 5.3.9.1	N/A	8F43	Change in the executing Firmware version	N/A	No	Security Log
SMETS1 4.3.9.1 SMETS1 5.3.9.1	N/A	8F44	Occurrence that has the potential to put Supply at risk and/or compromise the Integrity of the Device.	N/A	No	Security Log
SMETS1 4.3.9.1 SMETS1 5.3.9.1	N/A	8F60	Unusual numbers of malformed, out-of-order or unexpected Commands received	N/A	No	Security Log
SMETS1 4.3.9.1 SMETS1 5.3.9.1	N/A	8F45	Change of credit which is not reflective of normal Consumption	N/A	No	Security Log
SMETS1 4.3.9.1 SMETS1 5.3.9.1	N/A	8F46	Threat to Device security detected but not covered by other events.	N/A	No	Security Log
SMETS1 4.4.2.2 SMETS1 5.4.3.2	N/A	8F51	Duplicate UTRN entered	N/A	No	Security Log
SMETS1 4.4.2.2 SMETS1 5.4.3.2	N/A	8F63	UTRN not Authentic	N/A	No	Security Log
SMETS1 4.4.2 SMETS1 5.4.3	N/A	8161	User Interface Command Input and Successfully Actioned	N/A	No	Event Log
SMETS1 4.4.2 SMETS1 5.4.3	N/A	8162	User Interface Command Input but not Successfully Actioned	N/A	No	Event Log
SMETS1 4.4.3 SMETS1 5.4.4	N/A	8154	Immediate HAN Interface Command Received and Successfully Actioned	N/A	No	Event Log
SMETS1 4.4.3 SMETS1 5.4.4	N/A	8155	Immediate HAN Interface Command Received but not Successfully Actioned	N/A	No	Event Log

Table 2

8.3 SMETS1 Devices may additionally be capable of detecting events not required by SMETS1. Such additional events are referred to in this document as "SMETS1 Non-Mandated Events". Each such SMETS1 Non-Mandated Event may result in a log entry or an alert or both being created by the Device. For each such SMETS1 Non-Mandated Event, the DCC shall:

(a) produce a textual description of that event, such a description being referred to as a "SMETS1 Non-Mandated Event Description"; and

(b) associate a 16-bit integer where the most significant bit has the value zero and the integer is not associated with any other SMETS1 Non-Mandated Event Description. The hexBinary representation (with the meaning defined at http://www.w3.org/TR/xmlschema-2/#hexBinary) of this 16-bit integer shall be referred to as the "SMETS1 Non-Mandated Event Code".

8.4 The DCC shall maintain and publish to all Users the list of SMETS1 Non-Mandated Event Descriptions and, for each such description:

(a) the Device Type or Device Types which can detect such events;

(b) the associated SMETS1 Non-Mandated Event Code;

(c) whether, for each detected occurrence of the corresponding SMETS1 Non-Mandated Event, the DCC would produce a corresponding SMETS1 Alert and, if so, which User ID would be placed in the BusinessTargetID fields (with their Message Mapping Catalogue meanings);

(d) whether, for each detected occurrence of the corresponding SMETS1 Non-Mandated Event, a corresponding entry would appear in a SMETS1 Response containing the Device's Security Log (with its SMETS1 meaning); and

(e) whether, for each detected occurrence of the corresponding SMETS1 Non-Mandated Event, a corresponding entry would appear in a SMETS1 Response containing the Device's Event Log (with its SMETS1 meaning).

8.5 Each S1SP shall create a SMETS1 Alert whenever:

(a) it receives information that a SMETS1 Mandated Event or SMETS1 Non-Mandated Event has occurred; and

(b) a SMETS1 Alert is required for that Event (as identified in relation to SMETS1 Mandated Events in Table 2 above, or in relation to a SMETS1 Non-Mandated Event in accordance with the information published pursuant to Clause 8.4),

(c) unless it does not have a record of the User ID that it is to associate (pursuant to Table 2 or Clause 8.4(c)) with that Event/Alert Code, in which case it shall not create a SMETS1 Alert.

8.6 Where an S1SP creates a SMETS1 Alert based on information from a Device that a SMETS1 Mandated Event has occurred, the S1SP shall populate the GBCSHexadecimalMessageCode, GBCSHexAlertCode, and AlertDescription fields, and any BusinessTargetID fields (each with their Message Mapping Catalogue meanings) according to the values specified in Table 2 for the SMETS1 Mandated Event in question.

8.7 Where an S1SP creates a SMETS1 Alert based on information from a Device that a SMETS1 Non-Mandated Event has occurred, the S1SP shall populate:

(a) the GBCSHexadecimalMessageCode field (with its Message Mapping Catalogue meaning) with the SMETS1 Non-Mandated Event Message Code;

(b) the GBCSHexAlertCode field (with its Message Mapping Catalogue meaning) with the corresponding SMETS1 Non-Mandated Event Code;

(c) the AlertDescription field (with its Message Mapping Catalogue meaning) with the corresponding SMETS1 Non-Mandated Event Description; and

(d) any BusinessTargetID fields (with their Message Mapping Catalogue meanings) with the corresponding BusinessTargetID published pursuant to Clause 8.4(c).

8.8 Where an S1SP creates a SMETS1 Response which includes a log entry's details based on information from a Device that a SMETS1 Mandated Event has occurred, the S1SP shall populate the corresponding LogCode and LogDescription fields (with their Message Mapping Catalogue meanings) according to the values specified in Table 2 for the SMETS1 Mandated Event in question. Where an S1SP creates a SMETS1 Response which includes a log entry's details based on information from a Device that a SMETS1 Non-Mandated Event has occurred, the S1SP shall populate the corresponding LogCode and LogDescription fields (with their Message Mapping Catalogue meanings) according to the values specified in the document published by the DCC pursuant to Clause 8.3. An S1SP shall only include an entry in a SMETS1 Response containing details from a Security Log or an Event Log (with their SMETS1 meanings) where that entry relates to either a SMETS1 Mandated Event or a SMETS1 Non-Mandated Event.

8.9 An S1SP shall not include OtherInformation or OtherInformationLogMeaning fields (with their Message Mapping Catalogue meaning) in any SMETS1 Response.

9 SMETS1 Message Codes

9.1 Where an S1SP creates a SMETS1 Response, the S1SP shall

(a) identify the row in Table 3 where, in the corresponding Service Request:

(i) the Service Reference Variant has the value in the row; and

(ii) the Device Type recorded in the Smart Metering Inventory for the Device ID in the BusinessTargetID part of the RequestID (with their DUIS meanings) has the value in the row; and

(iii) Condition1 and Condition 2 (see Table 3) are true including, where relevant, in terms of the content of the corresponding Service Request;

(b) populate the GBCSHexadecimalMessageCode field (with its Message Mapping Catalogue meaning) according to the row identified at Clause 9.1(a); and

(c) include a Timestamp (with its Message Mapping Catalogue meaning) in the Header element (with its DUIS meaning) in the SMETS1 Response where the row identified at Clause 9.1(a) requires it.

Service Reference Variant	Type of target Device as recorded in the SMI	Condition 1	Condition 2	GBCSHexadecimalMessageCode	Timestamp required in SMETS1 Response Header?
1.1.1	ESME	True	True	0019	Yes
1.1.1	GSME	True	True	006B	Yes
1.2.1	ESME	True	True	00A2	Yes
1.2.1	GSME	True	True	00A3	Yes
1.5	ESME	If an AdjustMeterBalance element (with its DUIS meaning) is present	True	001C	No

Service Reference Variant	Type of target Device as recorded in the SMI	Condition 1	Condition 2	GBCSHexadecimalMessageCode	Timestamp required in SMETS1 Response Header?
1.5	GSME	If an AdjustMeterBalance element (with its DUIS meaning) is present	If a PrepaymentMode element (with its DUIS meaning) is present	0086	No
1.5	GSME	If an AdjustMeterBalance element (with its DUIS meaning) is present	If a CreditMode element (with its DUIS meaning) is present	00C0	No
1.5	ESME	If a ResetMeterBalance element (with its DUIS meaning) is present	True	00B3	No
1.5	GSME	If a ResetMeterBalance element (with its DUIS meaning) is present	If a PrepaymentMode element (with its DUIS meaning) is present	00B4	No
1.5	GSME	If a ResetMeterBalance element (with its DUIS meaning) is present	If a CreditMode element (with its DUIS meaning) is present	00C2	No
1.6	ESME	True	If a Prepayment element (with its DUIS meaning) is present	001B	Yes
1.6	ESME	True	If a Credit element (with its DUIS meaning) is present	001A	Yes
1.6	GSME	True	If a Prepayment element (with its DUIS meaning) is present	006D	Yes
1.6	GSME	True	If a Credit element (with its DUIS meaning) is present	006C	Yes
2.1	GSME	True	True	006F	Yes
2.1	ESME	True	True	00DE	Yes
2.2	ESME	True	True	0007	Yes
2.2	GSME	True	True	0097	Yes
2.3	ESME	True	True	001E	No

Service Reference Variant	Type of target Device as recorded in the SMI	Condition 1	Condition 2	GBCSHexadecimalMessageCode	Timestamp required in SMETS1 Response Header?
2.3	GSME	True	True	006E	No
2.5	ESME	True	True	0020	No
2.5	GSME	True	True	0070	No
3.2	ESME	True	True	0022	No
3.2	GPF	True	True	0072	No
3.3	GSME	True	True	0015	No
3.3	ESME	True	True	0024	No
4.1.1	ESME	True	True	0027	Yes
4.1.1	GSME or GPF	True	True	0074	Yes
4.1.2	ESME	True	True	0029	Yes
4.1.2	GSME or GPF	True	True	00B6	Yes
4.1.3	ESME	True	True	002A	Yes
4.1.4	GSME or GPF	True	True	00B8	Yes
4.2	ESME	True	True	0026	Yes
4.3	ESME	True	True	002D	Yes
4.3	GSME or GPF	True	True	0075	Yes
4.4.2	ESME	True	True	002F	No
4.4.2	GSME or GPF	True	True	00C3	No
4.4.3	ESME	True	True	0030	No
4.4.3	GSME or GPF	True	True	0076	No
4.4.4	ESME	True	True	002E	No
4.4.4	GSME or GPF	True	True	00C4	No
4.4.5	GSME or GPF	True	True	00C5	No
4.4.5	ESME	True	True	00C9	No
4.6.1	ESME	True	True	0033	No
4.6.1	GSME or GPF	True	True	0077	No
4.8.1	ESME	True	True	0037	No

Service Reference Variant	Type of target Device as recorded in the SMI	Condition 1	Condition 2	GBCSHexadecimalMessageCode	Timestamp required in SMETS1 Response Header?
4.8.1	GSME or GPF	True	True	0078	No
4.8.2	ESME	True	True	0038	No
4.8.3	ESME	True	True	0036	No
4.10	ESME	True	True	0039	Yes
4.10	GSME	True	True	0079	No
4.11.1	ESME	True	True	003A	No
4.11.1	GSME or GPF	True	True	009F	No
4.13	ESME	True	True	003B	No
4.13	GSME or GPF	True	True	00B5	No
4.15	ESME	True	True	0042	No
4.16	ESME	True	True	0028	Yes
4.18	ESME	True	True	0069	No
4.18	GSME or GPF	True	True	008D	No
6.2.1	ESME	True	True	003C	No
6.2.3	ESME	True	True	00D9	No
6.2.3	GSME or GPF	True	True	00DA	No
6.2.4	ESME	True	True	00F9	No
6.2.4	CHF	True	True	00FA	No
6.2.4	GSME	True	True	00FB	No
6.2.5	ESME	True	True	0040	No
6.2.8	GSME	True	True	007B	No
6.2.9	ESME	True	True	00BE	No
6.2.9	GSME or GPF	True	True	00BF	No
6.4.1	ESME	True	True	0043	Yes
6.4.2	ESME	True	True	0044	No

Service Reference Variant	Type of target Device as recorded in the SMI	Condition 1	Condition 2	GBCSHexadecimalMessageCode	Timestamp required in SMETS1 Response Header?
6.5	ESME	If RMSVoltageCountersNotReset (with its DUIS meaning) is not present	True	0045	No
6.5	ESME	If RMSVoltageCountersNotReset (with its DUIS meaning) is present	True	00D1	No
6.6	GSME	True	True	007C	No
6.7	GSME	True	True	007D	No
6.8	ESME	True	True	00D7	No
6.8	GSME	True	True	00D8	No
6.11	ESME	True	True	0062	No
6.11	GSME	True	True	007F	No
6.12	ESME	True	True	0047	No
6.13	GSME	If LogToRead (with its DUIS meaning) has the value 'Event'	True	0014	No
6.13	ESME	If LogToRead (with its DUIS meaning) has the value 'Event'	True	0048	No
6.13	ESME	If LogToRead (with its DUIS meaning) has the value 'Security'	True	0049	No
6.13	GSME	If LogToRead (with its DUIS meaning) has the value 'Security'	True	00A1	No
6.13	CHF	If LogToRead (with its DUIS meaning) has the value 'Event'	True	0093	No

Service Reference Variant	Type of target Device as recorded in the SMI	Condition 1	Condition 2	GBCSHexadecimalMessageCode	Timestamp required in SMETS1 Response Header?
6.13	CHF	If LogToRead (with its DUIS meaning) has the value 'Security'	True	0094	No
6.13	GPF	If LogToRead (with its DUIS meaning) has the value 'Event'	True	0014	No
6.13	GPF	If LogToRead (with its DUIS meaning) has the value 'Security'	True	00A1	No
6.13	GPF	If LogToRead (with its DUIS meaning) has the value 'GSMEEvent'	True	0014	No
6.13	GPF	If LogToRead (with its DUIS meaning) has the value 'GSMESecurity'	True	00A1	No
6.15.1	ESME or GPF	If RemotePartyRole (with its DUIS meaning) has the value 'NetworkOperator'	True	0103	Yes
6.15.1	ESME, GPF or GSME	If RemotePartyRole (with its DUIS meaning) has the value 'Supplier'	True	0102	Yes
6.21	ESME or GPF	If RemotePartyRole (with its DUIS meaning) has the value 'NetworkOperator'	True	0103	Yes
6.21	ESME, GPF or GSME	If RemotePartyRole (with its DUIS meaning) has the value 'Supplier'	True	0102	Yes
6.23	ESME, GPF or GSME	True	True	0107	Yes
6.24.1	ESME, GPF or GSME	True	True	0008	No

Service Reference Variant	Type of target Device as recorded in the SMI	Condition 1	Condition 2	GBCSHexadecimalMessageCode	Timestamp required in SMETS1 Response Header?
6.25	ESME	True	True	0068	No
6.27	ESME	True	True	00D3	No
7.1	ESME	True	True	004F	No
7.2	ESME	True	True	0050	No
7.2	GSME	True	True	0081	No
7.3	ESME	True	True	0051	No
7.3	GSME	True	True	0085	No
7.4	ESME	True	True	0052	No
7.4	GSME or GPF	True	True	0082	No
8.1.1	ESME	True	True	0062	No
8.1.1	GSME	True	True	007F	No
8.7.1	ESME	True	True	000D	No
8.7.1	GSME	True	True	00AF	No
8.7.2	ESME, GSME or GPF	True	True	000E	No
8.7.2	PPMID	If OtherDeviceID (with its DUIS meaning) contains a DeviceID which the SMI records as an ESME	True	00AB	No
8.7.2	PPMID	If OtherDeviceID (with its DUIS meaning) contains a DeviceID which the SMI records as an GSME	True	00AF	No
8.8.1	ESME or GSME	True	True	000F	No
8.8.2	PPMID	True	True	000F	No
8.8.2	ESME, GSME or GPF	True	True	0010	No
8.9	CHF	True	True	010F	No
8.11	CHF	If RequestType (with its DUIS meaning) is 'Add'.	True	0001	No

Service Reference Variant	Type of target Device as recorded in the SMI	Condition 1	Condition 2	GBCSHexadecimalMessageCode	Timestamp required in SMETS1 Response Header?
8.11	CHF	If RequestType (with its DUIS meaning) is 'Remove'	True	0002	No
11.2	ESME, PPMID or CHF	True	True	0059	No
11.2	GSME or GPF	True	True	0084	No
11.3	ESME, GSME, PPMID or CHF	True	True	0012	Yes

Table 3

9.2 Where a clause in section 17 or 18 relates to a SMETS1 GSME and, for the Service Request in question, where Table 3 allows that Service Request to be targeted at both a GSME and a GPF then that clause also applies in relation to a SMETS1 GPF.

10 Timestamp

10.1 Where an S1SP populates any Timestamp field (with its Message Mapping Catalogue meaning) in a SMETS1 Alert or a SMETS1 Response, the S1SP shall populate the field with a UTC value. The S1SP shall, if a corresponding timestamp is provided by the corresponding SMETS1 Device, base the value on the timestamp provided by the Device and shall, if a corresponding timestamp is not provided by the corresponding SMETS1 Device, base the value on the S1SP Time at the time the field is populated. Each S1SP shall ensure that its S1SP Time is accurate to within ten seconds of UTC.

11 Execution Counters

11.1 The DCC and each S1SP shall:

(a) maintain, for each SMETS1 Device of a Device Type in Table 4, a series of integers (the value of each of which shall be between 0 and (2^{64} -1) inclusive) as required by Table 4 dependent upon the type of the Device, as recorded in the Smart Metering Inventory (each such number being known as an "Execution Counter"); and

(b) before processing the first Service Request targeted at a specific SMETS1 Device, set all Execution Counters related to that SMETS1 Device to 0 except for the Execution Counters related to ‘Update Device Security Credentials (KRP) (SRV 6.15.1)’ which shall be set to (2^{64} -1).

Type of SMETS1 Device	**Required Execution Counters**
SMETS1 CHF	One for the ‘Activate Firmware (SRV 11.3)’ Service Request
SMETS1 PPMID	One for the ‘Activate Firmware (SRV 11.3)’ Service Request
SMETS1 ESME	One for each type of Critical Service Request which can be targeted at the Device (where type is defined by the Service Reference Variant value), excluding the ‘Update Device Security Credentials (KRP) (SRV 6.15.1). Two for the ‘Update Device Security Credentials (KRP) (SRV 6.15.1)’ Service Request: • One for use where RemotePartyRole is Supplier (with their DUIS meanings); and • One for use where RemotePartyRole is NetworkOperator (with their DUIS meanings). Two for the ‘Request Handover of DCC Controlled Device (SRV 6.21)’ Service Request: • One for use where RemotePartyRole is Supplier (with their DUIS meanings); and • One for use where RemotePartyRole is NetworkOperator (with their DUIS meanings). One for the ‘Top Up Device (SRV 2.2)’ Service Request
SMETS1 GSME	One for each Critical Service Request which can be targeted at the Device One for the ‘Request Handover of DCC Controlled Device (SRV 6.21)’ Service Request: which, for clarity, shall only be for use where RemotePartyRole is Supplier (with their DUIS meanings); and One for the ‘Top Up Device (SRV 2.2)’ Service Request

Type of SMETS1 Device	Required Execution Counters
SMETS1 GPF	Two for the 'Update Device Security Credentials (KRP) (SRV 6.15.1)' Service Request: • One for use where RemotePartyRole is Supplier (with their DUIS meanings); and • One for use where RemotePartyRole is NetworkOperator (with their DUIS meanings). Two for the 'Request Handover of DCC Controlled Device (SRV 6.21)' Service Request: • One for use where RemotePartyRole is Supplier (with their DUIS meanings); and • One for use where RemotePartyRole is NetworkOperator (with their DUIS meanings).
Other SMETS1 Device Types	None required

Table 4

11.2 The DCC and each S1SP shall:

(a) maintain, for each User which has a User Role of Import Supplier or Gas Supplier, a series of 1,000 integers (the value of each of which shall be between 0 and (2^{64} -1) inclusive) (each such number being known as a CoS Execution Counter); and

(b) before processing the first Service Request from such a User, set the CoS Execution Counter related to that User to 0.

12 Replay

12.1 Where the DCC or an S1SP is required to ensure that a Service Request is not a Replay, it shall, in the following order:

(a) Where the Service Request is not an 'Update Security Credentials (CoS) (SRV 6.23)' or a 'Request Handover of DCC Controlled Device (SRV 6.21)' Service Request, confirm that the User ID in the BusinessOriginatorID field (with its DUIS meaning) in the Service Request is the Notified Critical Supplier ID or the Notified Critical Network Operator ID (as the context requires) for, or where the Device Type of the target Device is

'CHF' or ‘PPMID’ the Notified Critical Supplier ID for the ESME Associated with, the Device whose Device ID is in the BusinessTargetID field (with its DUIS meaning) in the Service Request. Where that test fails, the Service Request shall be a Replay, processing of subsequent checks under this Clause shall not be undertaken and, if the test is being undertaken by an S1SP, the S1SP shall send an S1SP Alert accordingly.

(b) Where the Service Request is a ‘Update Security Credentials (CoS) (SRV 6.23)’ Service Request, confirm that the OriginatorCounter in the Service Request (with its DUIS meaning) is:

(i) greater than at least one of the CoS Execution Counter values that it holds for the sending User; and

(ii) is not equal to any of the CoS Execution Counter values that it holds for the sending User.

Where either of those tests fail, the Service Request shall be a Replay, and, if the tests are being undertaken by an S1SP, the S1SP shall send an S1SP Alert accordingly. Where both the tests succeed, the lowest of the CoS Execution Counter values for this User shall be replaced with the value of the OriginatorCounter in the Service Request (with its DUIS meaning).

(c) Where the Service Request is either a ‘Update Device Security Credentials (KRP) (SRV 6.15.1)’ or a ‘Request Handover of DCC Controlled Device (SRV 6.21)’ Service Request, confirm that the OriginatorCounter in the Service Request (with its DUIS meaning) is strictly numerically greater than the Execution Counter held for the Device ID is in the BusinessTargetID field (with its DUIS meaning) and the same RemotePartyRole as in the Service Request (with its DUIS meaning). Where that test fails, the Service Request shall be a Replay and, if the test is being undertaken by an S1SP, the S1SP shall send an S1SP Alert accordingly. Where the test succeeds the relevant Execution Counter value shall be replaced with the value of the OriginatorCounter in the Service Request (with its DUIS meaning).

(d) Where the Service Request is neither a ‘Update Device Security Credentials (KRP) (SRV 6.15.1)’ nor a ‘Request Handover of DCC Controlled Device (SRV 6.21)’ nor a ‘Update Security Credentials (CoS) (SRV 6.23)’ Service Request, confirm that the OriginatorCounter in the Service Request (with its DUIS meaning) is strictly numerically greater than the Execution Counter held for the Device ID is in the BusinessTargetID field (with its DUIS meaning) for this type of Service Request. Where that test fails, the Service Request shall be a Replay and, if the test is being undertaken by an S1SP, the S1SP shall send an S1SP Alert accordingly. Where the test succeeds the relevant Execution Counter value shall be replaced with the value of the OriginatorCounter (with its DUIS meaning) in the Service Request.

13 Configuration pre-requisites for operating a SMETS1 Device through the DCC

13.1 Some SMETS1 Devices may support features which are additional to those required by SMETS1 and which cannot be configured through the DCC. Table 5 lays out a number of such features. Where a Device supports, or is capable of supporting, one or more of the features in Table 5, the Responsible Supplier shall (unless to do so would result in a material delay to the Migration of the relevant SMETS1 Installation), ensure that before the relevant SMETS1 Installation is Migrated, any such features are configured according to the requirements of Table 5.

Feature	Type of Device	Required configuration
Privacy PIN which has to be entered to access SMETS information on the Device's user interface.	SMETS1 ESME, SMETS1 GSME	The Device shall be configured such that a PIN does not have to be entered to gain access to SMETS information on the Device's user interface, and such that the Energy Consumer cannot subsequently set such a PIN.
'Blacklisting' of access to the HAN	SMETS1 CHF	The Device shall be configured so that only 'whitelisted' Devices recorded on the SMI as being associated with the SMETS1 CHF can have access to the HAN, and that access is not controlled via any 'blacklisting' mechanism.
Configuration of actions to be taken on the occurrence of SMETS1 Mandated Events.	SMETS1 ESME, SMETS1 GSME	The Device shall be configured so that a Security Log or Event Log entry is created on occurrence of the SMETS1 Mandated Event where required by Table 2 and information is capable of being provided by the Device to the relevant S1SP to allow the S1SP to create any corresponding SMETS1 Alert, where required by Table 2.
Additional functionality not meant for Energy Consumer use, such as that available for installing engineers.	Any SMETS1 Device	The Device shall be configured so that Energy Consumers cannot access such facilities so for example, including the setting of any associated PINs or passwords so that they do not have default values.
Supplier name and / or contact details that may be visible to the Energy Consumer	Any SMETS1 Device	The Device shall be configured so that such values are either blank or not capable of being displayed to the Energy Consumer.
MPAN (ESME) or MPRN (GSME) whose value can be accessed via the Device's user interface or via the home area network.	SMETS1 ESME, SMETS1 GSME	The Device shall be configured so that such values are either blank or correctly identify the Metering Point for which the Smart Meter in question is measuring supply of energy in to the Premises.
Display of Currency Units	SMETS1 ESME SMETS1 GSME SMETS1 IHD SMETS1 PPMID	The Device shall be configured so that Currency Units (with its SMETS1 meaning) are displayed as GBP.

Remote energy supply control functionality	SMETS1 ESME SMETS1 GSME	The Device shall be configured so that Enable Supply, Disable Supply and Arm Load Switch (with their SMETS1 meanings) functions operate on receipt of the relevant instruction.

Table 5

13.2 For Category 1 Devices, the Responsible Supplier shall additionally ensure that, before the relevant SMETS1 Installation is Migrated, the Devices are configured according to the requirements in Table 15 in Annex B – Device Configuration Settings for Category 1 Devices.

14 Remote Party Role

14.1 Where a Remote Party Role Code is required in a Certificate or a Certificate Signing Request, the DCC shall use the Remote Party Role of 's1SPxmlSigning' (with its meaning in the Organisation Certificate Policy) when the Certificate or Certificate Signing Request relates to the DCC acting in the role of an S1SP.

15 SMETS1 Data Items

15.1 When a User creates a SMETS1 Service Request containing a field in Table 6, the User shall populate that field according to the meanings in Table 6.

DUIS / Message Mapping Catalogue field	**Meaning of values**
SuspendDebtDisabled	For an ESME: • **true**: shall mean that, if the Supply is Disabled (with its SMETS1 Meaning) pursuant to SMETS1 5.3.6.2, then the ESME shall suspend Time-based Debt Recovery. • **false**: shall mean that, if the Supply is Disabled (with its SMETS1 Meaning) pursuant to SMETS1 5.3.6.2, then the ESME shall continue with Time-based Debt Recovery For a GSME: • **true**: shall mean that, if the Supply is Disabled (with its SMETS1 Meaning) pursuant to SMETS1 4.3.6.2, then the GSME shall suspend Time-based Debt recovery.

	- **false**: shall mean that, if the Supply is Disabled (with its SMETS1 Meaning) pursuant to SMETS1 4.3.6.2, then the GSME shall continue with Time-based Debt Recovery
SuspendDebtEmergency	- **true**: shall mean that, if Emergency Credit (with its SMETS1 Meaning) is in use, then the Device shall suspend Time-based Debt Recovery. - **false**: shall mean that, if Emergency Credit (with its SMETS1 Meaning) is in use, then the Device shall continue with Time-based Debt Recovery
SupplyDepletionState	- **Locked**: shall have the SMETS1 meaning of Disabled - **Unchanged**: shall have the SMETS1 meaning of Unchanged
SupplyTamperState	- **Locked**: shall have the SMETS1 meaning of Disabled - **Unchanged**: shall have the SMETS1 meaning of Unchanged

Table 6

15.2 When an S1SP creates a SMETS1 Service Response containing a field in Table 6, the S1SP shall populate that field according to the meanings in Table 6.

15.3 When an S1SP creates a SMETS1 Service Response containing a field in Table 7, the S1SP shall populate that field according to the meanings in Table 7.

Message Mapping Catalogue field	**Meaning**
AccumulatedDebtRegister within ReadInstantaneousPrepayValuesRsp	Shall populate the field according to the SMETS1 meaning of Accumulated Debt Register, with the value being an integer value in thousandths of pence. For clarity, this is different that the SMETS2+ meaning of the same term.

Message Mapping Catalogue field	Meaning
AccumulatedDebtRegister within PrepaymentOperationalData	Shall populate the field according to the SMETS1 required Billing Data Log recording of the Accumulated Debt Register value, with the value being an integer value in thousandths of pence. For clarity, this is different that the SMETS2+ meaning of the same term.
Value within ConsumptionRegister	Shall populate the field according to the SMETS1 meaning of Total Consumption Register, with the value being a decimal number in metres cubed
GasActiveImportRegisterConsumption	Shall populate the field according to the SMETS1 required Daily Read Log copy of the Total Consumption Register, with the value being a decimal number in metres cubed
PrimaryValue within Gas	Shall populate the field according to the SMETS1 required Profile Data Log copy of the Total Consumption Register, with the value being a decimal number in metres cubed
Value within ActiveImportRegister	Shall populate the field according to the SMETS1 meaning of Total Active Import Register with the value being an integer number of watt hours (Wh).
ElecActiveImportRegisterConsumption	Shall populate the field according to the SMETS1 required Daily Read Log copy of the Total Active Import Register with the value being an integer number of watt hours (Wh).
PrimaryValue within Electricity	Shall populate the field according to the SMETS1 required Profile Data Log copy of the Total Active Import Register with the value being an integer number of watt hours (Wh).
Value within ReactiveImportRegister	Shall populate the field according to the SMETS1 Total Reactive Import Register with the value being an integer number of volt-amperes reactive hours (varh).
ReactiveEnergyImportedValue	Shall populate the field according to the SMETS1 required Profile Data Log copy of the Total Reactive Import Register with the value being an integer number of volt-amperes reactive hours (varh).

Message Mapping Catalogue field	Meaning
Value within ActiveExportRegister	Shall populate the field according to the SMETS1 meaning of Total Active Export Register with the value being an integer number of watt hours (Wh).
ActiveEnergyExportedValue	Shall populate the field according to the SMETS1 required Profile Data Log copy of the Total Active Export Register with the value being an integer number of watt hours (Wh).
Value within ReactiveExportRegister	Shall populate the field according to the SMETS1 meaning of Total Reactive Export Register with the value being an integer number of volt-amperes reactive hours (varh).
ReactiveEnergyExportedValue	Shall populate the field according to the SMETS1 required Profile Data Log copy of the Total Reactive Export Register with the value being an integer number of volt-amperes reactive hours (varh).
SupplyState	**Enabled** shall mean: • For a SMETS1 GSME, a Valve State of opened (with SMETS1 meanings); and • For a SMETS1 ESME, a Load Switch State of closed (with SMETS1 meanings) **Disabled** shall mean: • For a SMETS1 GSME, a Valve State of closed (with SMETS1 meanings); and • For a SMETS1 ESME, a Load Switch State of opened (with SMETS1 meanings) **Armed** shall mean: • For a SMETS1 GSME, a Valve State of armed (with SMETS1 meanings); and • For a SMETS1 ESME, a Load Switch State of armed (with SMETS1 meanings)

Table 7

16 OTA Header, Upgrade Image, OTA Upgrade Image and Authorising Remote Party Signature.

16.1 In relation to a Manufacturer Image which is to be sent to a Device, the Authorising Remote Party Signature shall be the Digital Signature generated across the Manufacturer Image using the private key associated with the Certificate identified by the Device's Notified Critical Supplier Certificate ID. Therefore the Authorising Remote Party Signature within an Upgrade Image can be checked (i.e. a Check Cryptographic Protection step may be carried out) using the Manufacturer Image and the Public Key in the Certificate identified by the Device's Notified Critical Supplier Certificate ID.

16.2 Upgrade Image shall be the concatenation:

Manufacturer Image || 0x0040 || Authorising Remote Party Signature

16.3 For clarity, each Manufacturer Image that is capable of being distributed using an Update Firmware Service Request must have an associated Central Products List entry containing a number of values. The OTA Header associated with that same Manufacturer Image shall be an octet string constructed using the values from that associated Central Products List entry in the way specified in Table 8, except that the OTA Header requires, in line with the ZigBee OTA specification, elements to be 'little endian'. Where Devices of this Device Model support the ZigBee OTA Specification, the values used shall also align to the corresponding values used by such Devices in OTA firmware related processing.

ZigBee OTA Message Element	Contents	Length (octets)	Note
OTA upgrade file identifier	0x0BEEF11E	4	
OTA Header version	0x0100	2	
OTA Header length	0x003C	2	
OTA Header Field control	0x0004	2	
Manufacturer code	Value of manufacturer_identifier in the associated Central Products List entry (with its Central Products List meaning)	2	Identifies the Manufacturer producing the Manufacturer Image
Image type	Value of model_identifier in the associated Central Products List entry (with its Central Products List meaning)	2	As per the ZigBee OTA specification, this is to differentiate products from the same Manufacturer
File version	Value of firmware_version in the associated Central Products List entry (with its Central Products List meaning)	4	As per the ZigBee OTA specification, this is to differentiate release and build numbers for the product in question
ZigBee Stack version	0x0002	2	
OTA Header string	Manufacturer specific	32	May be used but is not required to be used in Device processing of the Manufacturer Image
Total Image size (including header)	The length in octets of OTA Upgrade Image	4	Contents to be interpreted as an unsigned integer

Minimum hardware version	Value of hardware_version.version || hardware_version.revision in the associated Central Products List entry (with their Central Products List meanings)	2	
Maximum hardware version	Value of hardware_version.version || hardware_version.revision in the associated Central Products List entry (with their Central Products List meanings)	2	

Table 8

16.4 OTA Upgrade Image shall be the concatenation:

OTA Header || Upgrade Image

16.5 For each SMETS1 CHF, each SMETS1 PPMID, each SMETS1 ESME and each SMETS1 GSME with which the S1SP can (in each case) communicate, the S1SP shall maintain a Most Recently Verified Manufacturer Image Hash which shall be a 256-bit integer value and which shall be set to the value zero prior to the time at which the S1SP first communicates with the Device in question.

17 Processing SMETS1 Service Requests

17.1 The obligation on DCC to carry out Equivalent Steps when processing SMETS1 Service Requests shall be interpreted in light of the different requirements and device functionality set out in this document generally and in particular in these Clauses 17 and 18. In each case, the text describing the modified processing to be undertaken by DCC (including, where appropriate the relevant S1SP) relates to the type of Service Request(s) identified by Service Reference Variant in the underlined heading immediately above the text.

17.2 The different requirements and device functionality specified in Clause 17 shall apply to all SMETS1 Devices of the relevant Device Types.

17.3 The different requirements and device functionality specified in Clause 18 shall apply only to SMETS1 Devices which are of specified Device Models. Such Device Models and the different requirements or functionality that applies to them shall be specified in Annex A - Device Model Variations to Equivalent Steps Matrix (DMVES Matrix).

General

17.4 Where processing Service Requests that are requesting the reading of logs, and where, according to the Smart Metering Inventory, the target Device is a GSME, then the S1SP shall populate SMETS1 Responses using only data provided from the SMETS1 GSME and Unsupported Values in fields required by this Clause 17.

17.5 Where processing Service Requests for the reading of gas related information, and, according to the Smart Metering Inventory, the target Device is a GPF, then the S1SP shall populate SMETS1 Responses using any data available for the SMETS1 GSMS of which the SMETS1 GPF forms a part.

17.6 The DCC shall not be required to provide Enrolment or Communication Services in relation to any SMETS1 GSME that is added to the CHF Device Log of an Enrolled SMETS1 Smart Metering System.

17.6A Where Service Requests are attempting to write Configuration data (with its SMETS1 meaning) and are targeted at the SMETS1 GSME or SMETS1 GPF, any SMETS1 Responses will be triggered on receipt of the Service Request and not after processing on the device.

17.6B Clause 17.6A does not apply for Category 1 devices.

Update Tariff (SRV 1.1.1) and Update Price (SRV 1.2.1)

17.7 SMETS1 Smart Meters are not required to support Currency Units as a Configuration Data Item (with their SMETS2 meanings). Therefore, the S1SP shall discard any value in the CurrencyUnits fields (with its DUIS meaning) when setting values on the Smart Meter as a result of such a Service Request. For clarity, this discarding of values shall not result in an error in the SMETS1 Response.

17.8 For SMETS1 GSME, processing shall include the SMETS1 required capture of information in to the Billing Data Log (with its SMETS1 meaning), and so may therefore not include capturing a value for the Total Consumption Register (with its SMETS1 meaning).

17.9 For SMETS1 ESME, processing shall include the SMETS1 required capture of information in to the Billing Data Log (with its SMETS1 meaning), and so may therefore not include capturing values for the Total Active Import Register (with its SMETS1 meaning) or the Tariff TOU Block Register Matrix (with its SMETS2 meanings).

Adjust Meter Balance (SRV 1.5)

17.10 Where the Device is not capable of supporting Reset Meter Balance (with its SMETS2 meaning), the S1SP shall create a SMETS1 Response indicating failure.

Update Payment Mode (SRV 1.6)

17.11 Processing shall include the SMETS1 required capture of information in to the Billing Data Log (with its SMETS1 meaning), and so may therefore not include capturing values for the Total Consumption Register, Total Active Import Register or the Tariff TOU Block Register Matrix (with their SMETS1 / SMETS2 meanings).

17.12 Processing shall, except where clause 18 specifies different processing, reflect the meanings of SuspendDebtDisabled and SuspendDebtEmergency in Clause 15.1 noting that Standing Charge (with its SMETS1 meaning) will continue to be collected in all cases.

Update Prepay Configuration (SRV 2.1)

17.13 As per DUIS, processing shall not include the setting of values equivalent to the MaxMeterBalance and MaxCreditThreshold (with their DUIS meanings) where the Device does not support such setting.

Top Up Device (SRV 2.2)

17.14 Processing shall be as specified for an Add Credit WAN Interface Command (with their SMETS1 meanings).

Update Debt (SRV 2.3)

17.15 Where any one or more of TimeDebtRegister1, TimeDebtRegister2 and PaymentDebtRegister values (with their DUIS meanings) is not zero, debt adjustment related processing shall be as specified for an Adjust Debt WAN Interface Command (with their SMETS1 meanings). Other processing shall be as for a SMETS2+ Device.

Activate Emergency Credit (SRV 2.5)

17.16 Processing shall be as specified for an Activate Emergency Credit WAN Interface Command (with their SMETS1 meanings). As for a SMETS2+ Device, if, after the Device has executed the associated instructions, emergency credit is activated on the Device then the S1SP shall return a SMETS1 Response indicating the Command executed successfully. This shall be so regardless of whether emergency credit was activated on the Device prior to the instruction's execution or not except where Clause 18.8 applies.

Restrict Access For Change Of Tenancy (SRV 3.2)

17.17 Where, according to the Smart Metering Inventory, the target Device is an ESME, processing shall be as specified for a SMETS1 ESMS Restrict Data WAN Interface Command (with their SMETS1 meanings).

17.18 Where, according to the Smart Metering Inventory, the target Device is a GPF, processing shall be as specified for a SMETS1 GSMS Restrict Data WAN Interface Command (with their SMETS1 meanings).

Clear Event Log (SRV 3.3)

17.19 Processing shall be as specified for a Clear Event Log WAN Interface Command (with their SMETS1 meanings) and, therefore, a corresponding Security Log entry (with its SMETS1 meaning) may not be created.

Read Instantaneous Import TOU With Blocks Matrices (4.1.3)

17.20 Where the Device is not capable of providing Tariff TOU Block Register Matrix values (with its SMETS2meaning), the S1SP shall set the corresponding values in the SMETS1 Response to the relevant Unsupported Values.

Retrieve Change Of Mode / Tariff Triggered Billing Data Log (4.4.2) and Retrieve Billing Calendar Triggered Billing Data Log (SRV 4.4.3)

17.21 Where the Device is not capable of recording the Total Consumption Register or Total Active Import Register values (with their SMETS1 meanings) in such log entries, the S1SP shall set the corresponding values in the SMETS1 Response to the relevant Unsupported Values.

17.22 SMETS1 ESME are not required to record Tariff TOU Block Register Matrix values (with their SMETS2 meaning) but are required to record the Tariff Block Counter Matrix values in the Billing Data Log (with their SMETS1 meanings). Therefore, the S1SP shall, where the target Device is recorded as being an ESME in the Smart Metering Inventory, populate the TariffTOUBlock[1..4]RegisterMatrixValue values (with their Message Mapping Catalogue meaning) with the Tariff Block Counter Matrix values from the Billing Data Log (with their SMETS1 meanings).

17.23 For clarity, SMETS1 does not require the recording of additional prepayment values to the timetable set out in the Billing Calendar.

Retrieve Import Daily Read Log (SRV 4.6.1)

17.24 SMETS1 ESME are not required to record Tariff TOU Block Register Matrix values (with their SMETS2 meaning) but are required to record the Tariff Block Counter Matrix values in the Daily Read Log (with their SMETS1 meanings). Therefore, the S1SP shall, where the target Device is recorded as being an ESME in the Smart Metering Inventory, populate the TariffTOUBlock[1..4]RegisterMatrixValues values (with their Message Mapping Catalogue meaning) with the Tariff Block Counter Matrix values from the Daily Read Log (with their SMETS1 meanings).

17.25 For clarity, SMETS1 Smart Meters need only support 14 entries in this log.

Read Tariff Primary Element (SRV 4.11.1)

17.26 In populating a SMETS1 Response, the S1SP shall:

(a) set CurrencyUnitsLabel to GBP and CurrencyUnitsName to Millipence (with their Message Mapping Catalogue meanings), since these values do not have to be supported by SMETS1 Devices;

(b) set the value of PrimaryActiveTariffPrice and PrimaryActiveTariffPriceScale (with their Message Mapping Catalogue meanings) to the relevant Unsupported Value, so indicating that these values do not have to be supported by SMETS1 Devices;

(c) Read Tariff Type (with its SMETS1 meaning) from the target SMETS1 Smart Meter to establish whether it is 'Time-of-use' or 'Time-of-use with Block' (with their SMETS1 meanings);

(d) where the target Device is, according to the Smart Metering Inventory, a SMETS1 ESME:

(i) if Tariff Type is 'Time-of-use', then set the values in TariffTOUPriceMatrix to those read from the Device and the values in TariffBlockPriceMatrix (with their Message Mapping Catalogue meanings) to the relevant Unsupported Values, to denote which values are in use and so which Tariff Type; or

(ii) if Tariff Type is 'Time-of-use with Block', then set the values in TariffBlockPriceMatrix to those read from the Device and the values in TariffTOUPriceMatrix (with their Message Mapping Catalogue meanings) to the relevant Unsupported Values, to denote which values are in use and so which Tariff Type; and

(e) where the target Device is, according to the Smart Metering Inventory, a SMETS1 GSME:

(i) if Tariff Type is 'Time-of-use', then set the values in TOUTariff to those read from the Device and omit the BlockTariff element (with their Message Mapping Catalogue meanings), to denote which values are in use and so which Tariff Type; or

(ii) if Tariff Type is 'Time-of-use with Block', then set the values in BlockTariff to those read from the Device and omit the TOUTariff element (with their Message Mapping Catalogue meanings), to denote which values are in use and so which Tariff Type.

<u>Read Prepayment Configuration SRV 4.13</u>

17.27 Where the SMETS1 Device does not support the setting of values equivalent to the MaxMeterBalance or MaxCreditThreshold values (with their Message Mapping Catalogue meanings), then the S1SP shall, in populating a SMETS1 Response, set the values to the relevant Unsupported Value.

Read Load Limit Data (SRV 4.15)

17.28 A SMETS1 ESME cannot support a Load Limit Period (with its SMETS2 meaning) since the equivalent period is fixed at 30 seconds in SMETS1. Therefore, when populating a SMETS1 Response the S1SP shall set the LoadLimitPeriod (with its Message Mapping Catalogue meaning) to the relevant Unsupported Value.

17.29 A SMETS1 ESME cannot support a Load Limit Restoration Period (with its SMETS2 meaning) since there is no equivalent SMETS1 functionality. Therefore, when populating a SMETS1 Response, the S1SP shall set the LoadLimitRestorationPeriod (with its Message Mapping Catalogue meaning) to the relevant Unsupported Value.

Read Network Data (SRV 4.10)

17.30 A SMETS1 ESME is only required to support setting of Average RMS Voltage Measurement Period (with its SMETS1 meaning) in minutes, whereas the SMETS2 equivalent can be set in seconds. Therefore, where the SMETS1 ESME does not support setting to a resolution of seconds, the value in the MeasurementPeriod within AvgRMSVoltageProfileDataLog (with their Message Mapping Catalogue meanings) may be a multiple of 60 rather than the number of seconds requested in a prior ‘Update Device Configuration (Voltage) (SRV 6.5)’ Service Request.

Read Device Configuration (Identity Exc MPxN) (SRV 6.2.4)

17.31 In populating the SMETS1 Response, the S1SP shall:

(a) not include MeterVariant or ModelType fields (with their Message Mapping Catalogue meanings), since those do not have to be supported by SMETS1 Devices; and

(b) only include ManufacturerIdentifier (with its Message Mapping Catalogue meaning) where the target SMETS1 Device has a Device Identifier (with its SMETS1 meaning) and, in this case, set the value of ManufacturerIdentifier (with its Message Mapping Catalogue meaning) to be the value returned by the target Device for its Device Identifier (with its SMETS1 meaning).

Read Device Configuration (Gas) (SRV 6.2.8)

17.32 Where the SMETS1 Device does not support the setting of values equivalent to the StabilisationPeriod or MeasurementPeriod values (with their Message Mapping Catalogue meanings), then the S1SP shall, in populating a SMETS1 Response, set the values to the relevant Unsupported Value.

Update Device Configuration (Load Limiting General Settings) (SRV 6.4.1)

17.33 As noted in Clauses 17.28 and 17.29, a SMETS1 ESME cannot support either a Load Limit Period (with its SMETS2 meaning) or a Load Limit Restoration Period (with its SMETS2 meaning). Therefore, the S1SP shall discard any values in the LoadLimitPeriod or LoadLimitRestorationPeriod fields (with their DUIS meanings) when setting values on the SMETS1 ESME as a result of such a Service Request. For clarity, this discarding of values shall not result in an error in the SMETS1 Response.

Update Device Configuration (Voltage) (SRV 6.5)

17.34 A SMETS1 ESME is only required to support setting of Average RMS Voltage Measurement Period (with its SMETS1 meaning) in minutes, whereas the SMETS2 equivalent can be set in seconds. Therefore, where the target SMETS1 ESME does not support setting to a resolution of seconds, the S1SP shall divide the value in the AverageRMSVoltageMeasurementPeriod (with its DUIS meaning) by 60, round up to the nearest integer and set the value of the Average RMS Voltage Measurement Period (with its SMETS1 meaning) to the integer number of minutes so calculated.

Update Device Configuration (SRV 6.7)

17.35 Where a SMETS1 GSME supports the setting of values equivalent to the StabilisationPeriod or MeasurementPeriod values (with their Message Mapping Catalogue meanings), then the S1SP shall instruct the Device to set such values. Where the Device does not support setting of such values, the S1SP cannot send such instructions to the Device and therefore shall not do so and the S1SP shall create a SMETS1 Response indicating failure.

Read Event Or Security Log (SRV 6.13)

17.36 For clarity, in populating the SMETS1 Response, the S1SP shall comply with the requirements of Clause 8.

Update Security Credentials (KRP) (SRV 6.15.1)

17.37 The S1SP shall undertake the processing required by Clause 19. For clarity, since the Service Request is not to effect a change of control, any value in the RemotePartyFloorSequenceNumber field shall be discarded.

Update Security Credentials (CoS) (SRV 6.23)

17.38 Where the DCC has successfully authenticated the Service Request, the DCC shall then set all the Execution Counters required by Table 9 for the target Device (and for a SMETS1 ESME, the SMETS1 CHF and any SMETS1 PPMID on the same home area network), according to the Device Type recorded for that target Device in the Smart Metering Inventory, to the value specified for that Execution Counter in Table 9.

17.39 The S1SP shall undertake the processing required by Clause 19. Where that processing is successful, the S1SP shall then set each Execution Counter required by Table 9 for the target Device (and for a SMETS1 ESME, the SMETS1 CHF and any SMETS1 PPMID on the same home area network), according to the Device Type recorded for that target Device in the Smart Metering Inventory, to the value specified for that Execution Counter in Table 9.

Type of SMETS1 Device	**Execution Counters**
SMETS1 ESME	Those for each Critical Service Request which can be targeted at the Device, excluding the ‘Update Device Security Credentials (KRP) (SRV 6.15.1) shall be set to the value in the SupplierFloorSequenceNumber field; That for the ‘Update Device Security Credentials (KRP) (SRV 6.15.1)’ Service Request, for use where RemotePartyRole is Supplier (with their DUIS meanings) shall be set to the value in the SupplierFloorSequenceNumber field; That for the ‘Top Up Device (SRV 2.2)’ Service Request shall be set to the value in the SupplierFloorSequenceNumber field; In relation to the SMETS1 CHF which is Associated with the SMETS1 ESME, that for the ‘Activate Firmware (SRV 11.3)’ Service Request shall be set to the value in the SupplierFloorSequenceNumber field;

	In relation to any SMETS1 PPMID which is on the same home area network as the SMETS1 ESME, that for the 'Activate Firmware (SRV 11.3)' Service Request shall be set to the value in the SupplierFloorSequenceNumber field; and That for the 'Request Handover of DCC Controlled Device (SRV 6.21)' Service Request, for use where RemotePartyRole is Supplier (with their DUIS meanings), shall be set to (2^{64} -1).
SMETS1 GSME	Those for each Critical Service Request which can be targeted at the Device shall be set to the value in the SupplierFloorSequenceNumber field; That for the 'Top Up Device (SRV 2.2)' Service Request shall be set to the value in the SupplierFloorSequenceNumber field; and That for the 'Request Handover of DCC Controlled Device (SRV 6.21)' Service Request, for use where RemotePartyRole is Supplier (with their DUIS meanings), shall be set to (2^{64} -1).
SMETS1 GPF	That for the 'Update Device Security Credentials (KRP) (SRV 6.15.1)' Service Request, for use where RemotePartyRole is Supplier (with their DUIS meanings) shall be set to the value in the SupplierFloorSequenceNumber field; and That for the 'Request Handover of DCC Controlled Device (SRV 6.21)' Service Request, for use where RemotePartyRole is Supplier (with their DUIS meanings), shall be set to (2^{64} -1).

Table 9

Retrieve Device Security Credentials (KRP) (SRV 6.24.1)

17.40 If (with their DUIS meanings):

(a) RemotePartyRole is Supplier and there is no recorded Notified Critical Supplier ID for the target Device; or

(b) RemotePartyRole is NetworkOperator and there is no recorded Notified Critical Network Operator ID for the target Device; or

(c) RemotePartyRole is neither NetworkOperator nor Supplier then the S1SP shall populate the SMETS1 Response with a single instance of RemotePartyDetails where the RemotePartyRole is as per the Service Request, StatusCode is trustAnchorNotFound and all other fields are omitted. Only otherwise shall the S1SP undertake the processing required in Clause 17.41 or 17.42 as required by RemotePartyRole.

17.41 Where RemotePartyRole is Supplier (with their DUIS meanings), the S1SP shall populate the SMETS1 Response as follows:

(a) populate a first instance of RemotePartyDetails where CertificateUsage is DigitalSigning, ExistingCertificateHash is that from the Certificate identified by Notified Critical Supplier Certificate ID, ExistingRemotePartyId is the Notified Critical Supplier ID, StatusCode is success and RemotePartyFloorSeqNumber has the value of the Execution Counter for 'Update Device Security Credentials (KRP) (SRV 6.15.1)' Service Request, for use where RemotePartyRole is Supplier (with their DUIS meanings); and

(b) populate a second instance of RemotePartyDetails where CertificateUsage is KeyAgreement, ExistingCertificateHash is that from the Certificate identified by Notified Non-Critical Supplier Certificate ID, ExistingRemotePartyId is the Notified Non-Critical Supplier ID, StatusCode is success and RemotePartyFloorSeqNumber has the value of the Execution Counter for 'Update Device Security Credentials (KRP) (SRV 6.15.1)' Service Request, for use where RemotePartyRole is Supplier (with their DUIS meanings).

17.42 Where RemotePartyRole is NetworkOperator (with their DUIS meanings), the S1SP shall populate the SMETS1 Response as follows:

(a) populate a first instance of RemotePartyDetails where CertificateUsage is DigitalSigning, ExistingCertificateHash is that from the Certificate identified by Notified Critical Network Operator Certificate ID, ExistingRemotePartyId is the Notified Critical Network Operator ID, StatusCode is success and RemotePartyFloorSeqNumber has the value of the Execution Counter for 'Update Device Security Credentials (KRP) (SRV 6.15.1)' Service Request, for use where RemotePartyRole is NetworkOperator (with their DUIS meanings); and

(b) populate a second instance of RemotePartyDetails where CertificateUsage is KeyAgreement, ExistingCertificateHash is that from the Certificate identified by Notified Non-Critical Network Operator Certificate ID, ExistingRemotePartyId is the Notified Non-Critical Network Operator ID, StatusCode is success and RemotePartyFloorSeqNumber has the value of the Execution Counter for 'Update Device Security Credentials (KRP) (SRV 6.15.1)' Service Request, for use where RemotePartyRole is NetworkOperator (with their DUIS meanings).

Request Handover Of DCC Controlled Device (SRV 6.21)

17.43 The S1SP shall undertake the processing required by Clause **19**. Where that processing is successful, the S1SP shall then set Execution Counter values it holds in relation to the target Device according to the requirements of Table 10 and the Device Type recorded for the target Device in the Smart Metering Inventory. Where the S1SP creates a SMETS1 Response indicating success, it shall include in that SMETS1 Response an ExecutionOutcome (with its Message Mapping Catalogue meaning) element populated according to the requirements of Table 11.1. Where the DCC receives the resulting SMETS1 Response indicating success, the DCC shall set Execution Counter values it holds in relation to the target Device according to the requirements of Table 10 and the Device Type recorded for the target Device in the Smart Metering Inventory.

Type of SMETS1 Device and RemotePartyRole	**Required Execution Counter settings**
SMETS1 ESME or SMETS1 GSME or SMETS1 GPF where RemotePartyRole is Supplier (with their DUIS meanings)	That for the ‘Update Device Security Credentials (KRP) (SRV 6.15.1)’ Service Request, for use where RemotePartyRole is Supplier (with their DUIS meanings), shall be set to zero; and That for the ‘Request Handover of DCC Controlled Device (SRV 6.21)’ Service Request, for use where RemotePartyRole is Supplier (with their DUIS meanings), shall be set to (2^{64} -1).
SMETS1 ESME or SMETS1 GPF where RemotePartyRole is NetworkOperator (with their DUIS meanings)	That for the ‘Update Device Security Credentials (KRP) (SRV 6.15.1)’ Service Request, for use where RemotePartyRole is NetworkOperator (with their DUIS meanings), shall be set to zero; and That for the ‘Request Handover of DCC Controlled Device (SRV 6.21)’ Service Request, for use where RemotePartyRole is NetworkOperator (with their DUIS meanings), shall be set to (2^{64} -1).

Table 10

Data Item (with its Message Mapping Catalogue meaning)	**Required value in a SMETS1 Response**
AuthorisingRemotePartyOriginatorCounter	As per Message Mapping Catalogue.

CredentialsReplacementMode	Shall be populated with: • ‘SupplierBySupplier’ when the RemotePartyRole (with its DUIS meaning) in the Service Request is ‘Supplier’ • ‘NetworkOperatorbyNetworkOperator’ when the RemotePartyRole (with its DUIS meaning) in the Service Request is ‘NetworkOperator’
RemotePartySeqNumberChange	Shall be populated according to the requirements of Table 12.2
ReplacementOutcome	For each replacement (with its DUIS meaning) in the Service Request, shall be populated according to the requirements of Table 13.3

Table 11.1

Data Item (with its Message Mapping Catalogue meaning)	**Required value in a SMETS1 Response**
RemotePartyRole	The RemotePartyRole (with its DUIS meaning) in the Service Request
RemotePartyFloorSeqNumber	The RemotePartyFloorSeqNumber (with its DUIS meaning) in the Service Request

Table 12.2

Data Item (with its Message Mapping Catalogue meaning)	**Required value in a SMETS1 Response**
StatusCode	‘success’
CertificateType	• ‘DigitalSigning’ for a ‘DigitalSigningCertificate’ (with its DUIS meaning) in the Service Request

	• ‘KeyAgreement’ for a ‘KeyAgreementCertificate’ (with its DUIS meaning) in the Service Request
RemotePartyRole	The RemotePartyRole (with its DUIS meaning) in the Service Request
ExistingRemotePartyID	• The subject unique identifier equating to Entity Identifier (64 bit value) of a valid SMKI Certificate with the Remote Party Role of ‘accessControlBroker’ and keyUsage of ‘digitalSignature’ for a ‘DigitalSigningCertificate’ (with its DUIS meaning) in the Service Request • The subject unique identifier equating to Entity Identifier (64 bit value) of a valid SMKI Certificate with the Remote Party Role of ‘accessControlBroker’ and keyUsage of ‘keyAgreement’ for a ‘KeyAgreementCertificate’ (with its DUIS meaning) in the Service Request
NewRemotePartyID	• The subject unique identifier equating to Entity Identifier (64 bit value) of the ‘DigitalSigningCertificate’ (with its DUIS meaning) in the Service Request • The subject unique identifier equating to Entity Identifier (64 bit value) of a ‘KeyAgreementCertificate’ (with its DUIS meaning) in the Service Request
ExistingCertificateHash	• The subject key identifier, a SHA-1 Hash of the public key contained ina valid SMKI Certificate with the Remote Party Role of ‘accessControlBroker’ and keyUsage of ‘digitalSignature’ for a ‘DigitalSigningCertificate’ (with its DUIS meaning) in the Service Request • The subject key identifier, a SHA-1 Hash of the public key contained in a valid SMKI Certificate with the Remote Party Role of ‘accessControlBroker’ and keyUsage of ‘keyAgreement’ for a ‘KeyAgreementCertificate’ (with its DUIS meaning) in the Service Request
NewCertificateHash	• The subject key identifier, a SHA-1 Hash of the public key contained in a ‘DigitalSigningCertificate’ (with its DUIS meaning) in the Service Request • The subject key identifier, a SHA-1 Hash of the public key contained in a ‘KeyAgreementCertificate’ (with its DUIS meaning) in the Service Request

Table 13.3

Enable Supply (SRV 7.1)

17.44 For clarity, this command in SMETS1 is unconditional unlike in SMETS2. Therefore, the Service Request may result in supply being enabled on a

SMETS1 Smart Meter when it would not be enabled on a SMETS2 Smart Meter which is in the same state.

Arm Supply (SRV 7.3)

17.45 On receipt of this Service Request, the S1SP shall create and send a SMETS1 Arm Valve (for SMETS1 GSME) or a SMETS1 Arm Load Switch (for SMETS1 ESME) command. For clarity, these commands in SMETS1 are unconditional unlike the equivalent command in SMETS2. Therefore, the Service Request may result in supply being armed on a SMETS1 Smart Meter when it would not be armed on a SMETS2 Smart Meter which is in the same state.

Join Service (Critical) (SRV 8.7.1) and Join Service (Non-Critical) (SRV 8.7.2)

17.46 If, according to the information held by the S1SP, the Devices identified by OtherDeviceID and by BusinessTargetID (with their DUIS meanings) are not both on the same SMETS1 CHF's 'SMETS1 CHF Device Log', the S1SP shall create a SMETS1 Response indicating failure; otherwise the S1SP shall create a SMETS1 Response indicating success.

Unjoin Service (Critical) (SRV 8.8.1) and Unjoin Service (Non-Critical) (SRV 8.8.2)

17.47 The S1SP shall create a SMETS1 Response indicating success.

Read Device Log (SRV 8.9)

17.48 In populating the SMETS1 Response, the S1SP shall:

(a) include a CHFDeviceLogEntry (with its Message Mapping Catalogue meaning) for the SMETS1 GPF which is within the same SMETS1 CH as the SMETS1 CHF to which this Service Request is targeted;

(b) include a CHFDeviceLogEntry (with its Message Mapping Catalogue meaning) for the SMETS1 ESME which is within the same SMETS1 ESMS as the SMETS1 CHF to which this Service Request is targeted; and

(c) include, except for the SMETS1 ESME, a CHFDeviceLogEntry (with its Message Mapping Catalogue meaning) for each SMETS1 Device which communicates via the home area network using ZigBee Alliance standards managed by the SMETS1 CHF to which this Service Request is targeted.

17.49 This set of Devices for which CHFDeviceLogEntry (with its Message Mapping Catalogue meaning) would be created shall be referred to as the SMETS1 CHF's 'SMETS1 CHF Device Log'.

17.50 In populating a CHFDeviceLogEntry (with its Message Mapping Catalogue meaning) in a SMETS1 Response for a particular Device, the S1SP shall:

(a) set the value of DeviceID (with its Message Mapping Catalogue meaning) to the Device's Device ID, where that Device ID complies with Clause 3;

(b) set the value of SubGHzLinkQuality (with its Message Mapping Catalogue meaning) to zero, meaning that the Device is not communicating on Sub GHz frequencies;

(c) where the Device is not able to support the LastCommunicationsDateTime (with its Message Mapping Catalogue meaning) parameter, set the value of that parameter to the relevant Unsupported Value, to indicate that it does not support that parameter; and

(d) where the Device is able to support the LastCommunicationsDateTime (with its Message Mapping Catalogue meaning) parameter, set the value of that parameter to a value equivalent to that returned by the Device.

<u>Update HAN Device Log (SRV 8.11)</u>

17.51 Where RequestType is Add (with their DUIS meanings), the S1SP shall undertake processing in the following sequence stopping at the point at which it creates a SMETS1 Response:

(a) where DeviceID in the UpdateHANDeviceLog element (with their DUIS meanings) is, according to the Smart Metering Inventory a SMETS1 GPF:

(i) if, according to the Smart Metering Inventory, the SMETS1 GPF is Associated with the target SMETS1 CHF, the S1SP shall create a SMETS1 Response indicating success; or

(ii) if, according to the Smart Metering Inventory, the SMETS1 GPF is not Associated with the target SMETS1 CHF, the S1SP shall create a SMETS1 Response indicating failure;

(b) where DeviceID in the UpdateHANDeviceLog element (with their DUIS meanings) is, according to the Smart Metering Inventory a SMETS1 ESME which the S1SP knows does not require connection to a ZigBee Specification based home area network to communicate with the SMETS1 CHF:

(i) if, according to the S1SP's information, the SMETS1 ESME forms part of the same SMETS1 ESMS as the SMETS1 CHF, the S1SP shall create a SMETS1 Response indicating success; or

(ii) if, according to the S1SP's information, the SMETS1 ESME does not form part of the same SMETS1 ESMS as the SMETS1 CHF, the S1SP shall create a SMETS1 Response indicating failure;

(c) where DeviceID in the UpdateHANDeviceLog element (with their DUIS meanings) does not meet the criteria at (a) or that at (b):

(i) if, according to the information available to S1SP, the Device is already on the SMETS1 CHF’s ‘SMETS1 CHF Device Log’, the S1SP shall create a SMETS1 Response indicating success; or

(ii) if, according to the information held by the S1SP, the Device is already on another SMETS1 CHF’s ‘SMETS1 CHF Device Log’, the S1SP shall create a SMETS1 Response indicating failure and indicating which other SMETS1 CHF the Device is Associated with; or

(iii) if the criteria at neither (i) nor (ii) are met, the S1SP shall:

(A) instruct the CHF to allow the Device identified by DeviceID (with its DUIS meaning) to join the home area network controlled by the SMETS1 CHF, using the InstallCode and JoinTimePeriod (with their DUIS meaning). For clarity, SMETS1 CHF may not support a configurable home area network joining period. Only where this is so, the S1SP shall discard any JoinTimePeriod value (with their DUIS meaning); and

(B) ascertain (allowing for any relevant latency in the joining process, including where relevant the JoinTimePeriod (with its DUIS meaning)) whether the Device identified by Device ID (with its DUIS meaning) has joined the home area network and so is able to communicate over it. If the Device is able to communicate over the home area network, the S1SP shall create a SMETS1 Response indicating success. If the Device is not able to communicate over the home area network, the S1SP shall create a SMETS1 Response indicating failure.

17.52 Where RequestType is Remove (with their DUIS meanings), the S1SP shall undertake processing in the following sequence stopping at the point at which it creates a SMETS1 Response:

(a) where DeviceID in the UpdateHANDeviceLog element (with their DUIS meanings) is, according to the Smart Metering Inventory a SMETS1 GPF, then the S1SP shall create a SMETS1 Response indicating failure; or

(b) where DeviceID in the UpdateHANDeviceLog element (with their DUIS meanings) is, according to the Smart Metering Inventory a SMETS1 ESME which the S1SP knows does not require connection to a ZigBee Specification based home area network to communicate with the SMETS1 CHF, then the S1SP shall create a SMETS1 Response indicating failure;

(c) where DeviceID in the UpdateHANDeviceLog element (with their DUIS meanings) does not meet the criteria at (a) or that at (b):

(i) if, according to the information available to S1SP, the Device is not already on the SMETS1 CHF's 'SMETS1 CHF Device Log', then the S1SP shall create a SMETS1 Response indicating success; or

(ii) if, according to the information available to S1SP, the Device is on the SMETS1 CHF's 'SMETS1 CHF Device Log', then the S1SP shall:

(A) instruct the SMETS1 CHF to stop the Device identified by DeviceID (with its DUIS meaning) from having access to the home area network controlled by the SMETS1 CHF, and instruct the SMETS1 CHF to confirm whether it has stopped such access; and

(B) where the S1SP receives a response from the SMETS1 CHF detailing successful removal of access within a period allowing for latency in the process, the S1SP shall create a SMETS1 Response indicating success. Otherwise, the S1SP shall create a SMETS1 Response indicating failure.

Update Firmware (SRV 11.1)

17.52AClauses 17.53 to 17.57 shall not apply when Clause 18.63(b) applies.

17.53 On receipt of a firmware distribution request from the DCC, the S1SP shall, for each Device identified in that request confirm that the Device:

(a) is one for which the S1SP is operationally responsible; and

(b) is, according to the Smart Metering Inventory, of the same Device Model, other than the firmware version element, as is specified by the corresponding four values in the OTA Header.

17.54 The S1SP shall notify the DCC of the list of Device IDs which fail the check at 17.53, and the DCC shall send a DCC Alert to the User that sent the original ‘Update Firmware’ Service Request.

17.54A In relation to Clauses 17.55 and 17.56 where the Device is a CHF or PPMID, references to the Notified Critical Supplier Certificate ID shall be interpreted as references to the Notified Critical Supplier Certificate ID of the ESME on the same home area network.

17.55 Where the S1SP does immediately distribute Manufacturer Images to Devices of the Device Model identified by the OTA Header, the S1SP shall, for each Device which passes the check at 17.53:

(a) if the Notified Critical Supplier Certificate ID is the same as that of a previous Device being processed where a Check Cryptographic Protection of the Authorising Remote Party Signature for that previous Device had succeeded, then:

(i) the S1SP shall distribute the Manufacturer Image to the Device and instruct the Device to confirm when it has successfully received that image; and

(ii) where the S1SP receives a response from the Device detailing successful reception within a period allowing for latency in the process, the S1SP shall create a SMETS1 Alert for this Device to alert ‘Firmware Verification Successful’ for this Device’s Device Type (according to the Smart Metering Inventory); otherwise, the S1SP shall create a SMETS1 Alert for this Device to alert ‘Firmware Verification Failed’ for this Device’s Device Type (according to the Smart Metering Inventory);

(b) if the Notified Critical Supplier Certificate ID is either (1) different than that of a previous Device being processed where a Check Cryptographic Protection of the Authorising Remote Party Signature for that previous Device had succeeded or (2) the same as that of a previous Device being processed where the check of Authorising Remote Party Signature for that previous Device had failed, then the S1SP shall create a SMETS1 Alert for this Device to alert ‘Firmware Verification Failed’ for this Device’s Device Type (according to the Smart Metering Inventory); and

(c) if no previous Device being processed has successfully passed the Check Cryptographic Protection of the Authorising Remote Party Signature, the S1SP shall undertake the check of Authorising Remote Party Signature for this Device using the Public Key in the Certificate identified by Notified Critical Supplier Certificate ID. If that check fails then the S1SP shall create a SMETS1 Alert for this Device to alert ‘Firmware Verification Failed’ for this Device’s Device Type (according to the Smart Metering Inventory); otherwise:

(i) the S1SP shall distribute the Manufacturer Image to the Device and instruct the Device to confirm when it has successfully received that image; and

(ii) where the S1SP receives a response from the Device detailing successful reception within a period allowing for latency in the process, the S1SP shall create a SMETS1 Alert for this Device to alert ‘Firmware Verification Successful’ for this Device’s Device Type (according to the Smart Metering Inventory); otherwise, the S1SP shall create a SMETS1 Alert for this Device to alert ‘Firmware Verification Failed’ for this Device’s Device Type (according to the Smart Metering Inventory).

17.56 Where the S1SP does not immediately distribute Manufacturer Images to Devices of the Device Model identified by the OTA Header, the S1SP shall retain the Manufacturer Image and, for each Device which passes the check at 17.53:

(a) if the Notified Critical Supplier Certificate ID is the same as that of a previous Device being processed where the check of Authorising Remote Party Signature for that previous Device had succeeded, the S1SP shall create a SMETS1 Alert for this Device to alert 'Firmware Verification Successful' for this Device's Device Type (according to the Smart Metering Inventory);

(b) if the Notified Critical Supplier Certificate ID is either (1) different to that of a previous Device being processed where the check of Authorising Remote Party Signature for that previous Device had succeeded or (2) the same as that of a previous Device being processed where the check of Authorising Remote Party Signature for that previous Device had failed, then the S1SP shall create a SMETS1 Alert for this Device to alert 'Firmware Verification Failed' for this Device's Device Type (according to the Smart Metering Inventory); and

(c) if no previous Device being processed has successfully passed the check of Authorising Remote Party Signature, the S1SP shall undertake the check of Authorising Remote Party Signature for this Device. If that check fails then the S1SP shall create a SMETS1 Alert for this Device to alert 'Firmware Verification Failed' for this Device's Device Type (according to the Smart Metering Inventory); otherwise the S1SP shall create a SMETS1 Alert for this Device to alert 'Firmware Verification Successful' for this Device's Device Type (according to the Smart Metering Inventory).

17.57 Whenever the S1SP creates a SMETS1 Alert for 'Firmware Verification Successful', the S1SP shall set the value of the Device's Most Recently Verified Manufacturer Image Hash to be the Hash of the associated Manufacturer Image.

Read Firmware Version (SRV 11.2)

17.58 Based on the information available to it, the S1SP shall populate the FirmwareVersion field (with its Message Mapping Catalogue meaning) with the value from the Central Products List's firmware_version field (with its Central Products List meaning), excluding any colons from the firmware_version field's value, that reflects the operating firmware version for the Device's Device Model.

Activate Firmware (SRV 11.3)

17.59 If the FirmwareHash value (with its DUIS meaning) is not the same as the target Device's Most Recently Verified Manufacturer Image Hash, the S1SP shall create a SMETS1 Response indicating failure.

17.60 If the FirmwareHash value (with its DUIS meaning) is the same as the target Device’s Most Recently Verified Manufacturer Image Hash:

(a) the S1SP shall instruct the Device to activate the Manufacturer Image (if necessary for the Device Model, by distributing the Manufacturer Image to it) and instruct the Device to confirm when it has successfully activated that Manufacturer Image; and

(b) where the S1SP receives a response from the Device detailing successful activation within a period allowing for latency in the process, the S1SP shall create a SMETS1 Response indicating success; otherwise, the S1SP shall create a SMETS1 Response indicating failure.

Synchronise Clock (SRV 6.11) and Commission Device (SRV 8.1.1)

17.61 Where the target Device is capable of maintaining time independently of any other Device in the Smart Metering System, the S1SP shall determine the Device’s time and, if the Device’s time is within the period defined by CurrentDateTime and CurrentDateTime plus TolerancePeriod (with their DUIS meanings), the S1SP shall return a SMETS1 Response indicating ‘reliable’. If the Device’s time can be determined but is outside of that period, the S1SP shall return a SMETS1 Response indicating ‘unreliable’. If the S1SP determines that the Device does not have a valid time, the S1SP shall return a SMETS1 Response indicating ‘invalid’.

17.62 Where the target Device is not capable of maintaining time independently of another Device in the Smart Metering System, the S1SP shall determine the time of the Device that serves as the time source for the target Device and, if the time source Device's time is within the period defined by CurrentDateTime and CurrentDateTime plus TolerancePeriod (with their DUIS meanings), the S1SP shall return a SMETS1 Response indicating 'reliable'. If the time source Device's time can be determined but is outside of that period, the S1SP shall return a SMETS1 Response indicating 'unreliable'. If the S1SP determines that the Device does not have a valid time, the S1SP shall return a SMETS1 Response indicating 'invalid'.

18 Processing SMETS1 Service Requests – Device specific behaviour

18.1 Update Import Tariff (Primary Element) (SRV 1.1.1)

(a) Where the target SMETS1 ESME does not support a Standing Charge (with its SMETS1 meaning) with an accuracy of greater than hundred thousandths of Currency Units (with its SMETS1 meaning) per day, the S1SP shall, where the Service Request specifies a StandingChargeScale (with its DUIS meaning) of -6 or less, create a SMETS1 Response indicating failure.

(b) Where the target SMETS1 ESME does not support prices in a Tariff TOU Price Matrix or Tariff Block Price Matrix (with its SMETS1 meaning) with an accuracy of greater than hundred thousandths of Currency Units (with its SMETS1 meaning) per kWh, the S1SP shall, where the Service Request specifies a PriceScale (with its DUIS meaning) of -6 or less, create a SMETS1 Response indicating failure.

(c) Where the target SMETS1 ESME does not support a Standing Charge (with its SMETS1 meaning) with an accuracy of greater than ten thousandths of Currency Units (with its SMETS1 meaning) per day and the StandingChargeScale (with its DUIS meaning) specified is -5, the S1SP shall round the Standing Charge value (with its SMETS1 meaning) down to whole numbers of ten thousandths of Currency Units (with its SMETS1 meaning) per day.

(d) Where the target SMETS1 ESME does not support a PriceScale (with its DUIS meaning) at a resolution greater than ten thousandths of Currency Units (with its SMETS1 meaning) per kWh and the PriceScale (with its DUIS meaning) specified is -5, the S1SP shall round down the value of all prices in the Service Request to whole numbers of ten thousandths of Currency Units (with its SMETS1 meaning) per kWh.

(e) Where the SMETS1 ESME or SMETS1 GSME does not support StandingCharge (with its DUIS meaning) that is larger than 32767 and the StandingCharge (with its DUIS meaning) is greater than this value, the S1SP shall repeatedly divide the value by 10 and increase the associated scale by 1 until the resulting value can be stored on the Device. The stored value shall be rounded down to the nearest integer if the value to store is no longer an integer after rescaling.

(f) Where the SMETS1 ESME or SMETS1 GSME does not support prices in the TariffTOUPriceMatrix or TariffBlockPriceMatrix (with their DUIS meanings) that are larger than 32767 and any of the values in TariffTOUPriceMatrix or TariffBlockPriceMatrix (with their DUIS meanings) is greater than this value, the S1SP shall repeatedly divide all the values by 10 and increase the associated scale by 1 until the all the resulting values can be stored on the device. The stored values shall be rounded down to the nearest integer if the values to store are no longer integers after rescaling.

(g) Where the target SMETS1 ESME does not support simultaneous setting of Tariff Type (with its SMETS1 meaning) of 'Time-of-use' and 'Time-of-use with Block' and where HybridTariff (with its DUIS meaning) is specified, the S1SP shall create a SMETS1 Response indicating failure.

(h) Where the target SMETS1 GSME does not support more than two seasons in the Tariff Switching Table (with its SMETS1 meaning) and GasSeasons (with its DUIS meaning) specifies three seasons, the S1SP shall create a SMETS1 Response indicating failure.

(i) Where the target SMETS1 GSME does not support the equivalent of wildcards in the SeasonStartDate fields or the Date field in a GasSpecialDay fields (with their DUIS meanings), the S1SP shall, where the Service Request specifies such wildcards, create a SMETS1 Response indicating failure.

(j) Where the Service Request specifies a StandingCharge (with its DUIS meaning) greater than 32767 millipence and the target SMETS1 GSME does not support such a value, the S1SP shall create a SMETS1 Response indicating failure.

(k) Where the SMETS1 ESME is capable of switching an Auxiliary Load Control Switch (with its SMETS2 meaning) Where the SMETS1 ESME is capable of switching an Auxiliary Load Control Switch (with its SMETS2 meaning) according to a schedule that may only be configured in conjunction with the configuration of the Tariff Switching Table (with its SMETS1 meaning); and

(i) where TOUTariff (with its DUIS meaning) is present in the Service Request;

(ii) where all DayProfile (with its DUIS meaning) elements reference the same two TOUPrice (with its DUIS meaning) indices and no others;

(iii) those two TOUPrice's (with its DUIS meaning) values differ; and

(iv) where the Year of a Season StartDate (with their DUIS meanings) is given as a wildcard

then the S1SP shall configure the ESME to have the effect that, the Auxiliary Load Control Switch is, for the applicable DayProfile(s), closed at the StartTime(s) that reference the TOUPrice with the lowest value and is open at the StartTime(s) that reference the TOUPrice with the highest value (all with their DUIS meanings). Where conditions (i), (ii) and (iii) are not met, then the S1SP shall configure the ESME to have the effect that the state of the Auxiliary Load Control Switch is open at all times.

(l) Where the SMETS1 ESME is capable of switching an Auxiliary Load Control Switch (with its SMETS2 meaning) according to a schedule that may only be configured in conjunction with the configuration of the Tariff Switching Table (with its SMETS1 meaning); and

(i) where TOUTariff (with its DUIS meaning) is present in the Service Request;

(ii) where all DayProfile (with its DUIS meaning) elements reference the same two TOUPrice (with its DUIS meaning) indices and no others; and

(iii) those two TOUPrice's (with its DUIS meaning) values differ;

then the S1SP shall configure the ESME to have the effect that, the Auxiliary Load Control Switch is, for the applicable DayProfile(s), closed at the StartTime(s) that reference the TOUPrice with the lowest value and is open at the StartTime(s) that reference the TOUPrice with the highest value (all with their DUIS meanings). Where conditions (i), (ii) and (iii) are not met, then the S1SP shall configure the ESME to have the effect that the state of the Auxiliary Load Control Switch is open at all times.

(m) Where the target SMETS1 ESME does not support the setting of a tariff where:

(i) the SeasonStartDate has a SpecifiedYear;

(ii) the SeasonStartDate has a NonSpecifiedMonth;

(iii) the SeasonStartDate has a NonSpecifiedDayofMonth, or a LastDayofMonth or a SecondLastDayofMonth;

(iv) the SeasonStartDate has a SpecifiedDayofWeek;

(v) any of the SpecialDays has a NonSpecifiedDayofMonth, or a LastDayofMonth or a SecondLastDayofMonth;

(vi) any of the SpecialDays has a NonSpecifiedMonth;

(vii) any of the SpecialDays hasa SpecifiedDayofWeek;

(viii) the earliest StartTime (with its DUIS meaning) in each DayProfile (with its DUIS meaning) is other than midnight (UTC);

(ix) where any of the StartTimes (with their DUIS meanings) are not the start of minutes 00 or 30 in any hour or

(x) the order of the XML elements within the Seasons XML element is other than in ascending order of the SeasonStartDate (with their DUIS meanings)

then the S1SP shall, where it receives a Service Request that does not meet these criteria, create a SMETS1 Response indicating failure.

(n) Where the target SMETS1 GSME does not support the setting of a tariff where:

(i) the SeasonStartDate has a SpecifiedYear;

(ii) the SeasonStartDate has a NonSpecifiedMonth;

(iii) the SeasonStartDate has a NonSpecifiedDayofMonth;

(iv) the SeasonStartDate has a SpecifiedDayofWeek;

(v) any of the SpecialDays has a NonSpecifiedDayofMonth;

(vi) any of the SpecialDays has a NonSpecifiedMonth;

(vii) any of the SpecialDays has a SpecifiedDayofWeek;

(viii) the order of the XML elements within the Seasons XML element is other than in ascending order of the SeasonStartDate (with their DUIS meanings)

then the S1SP shall, where it receives a Service Request that does not meet these criteria, create a SMETS1 Response indicating failure.

(o) Where the target SMETS1 ESME does not support the setting of a tariff where:

(i) the SeasonStartDate has a SpecifiedYear;

(ii) the SeasonStartDate has a SpecifiedDayofWeek;

then the S1SP shall discard any SpecifiedYear or SpecifiedDayofWeek values (with their DUIS meanings) and configure the Device as if those values were NonSpecifiedYear or NonSpecifiedDayofWeek.

(p) For such SMETS1 ESME, the S1SP shall set any prices, not specified in whichever of BlockTariff or TOUTariff (with their DUIS meanings) is present in the Service Request, to zero in its instructions to the Device.

(q) For such SMETS1 GSME, the S1SP shall, where BlockTariff (with its DUIS meaning) is present in the Service Request, set any prices, not specified in the Service Request, to zero in its instructions to the Device.

(r) Where the target SMETS1 GSME does not support the setting of a tariff where:

(i) the SeasonStartDate has a NonSpecifiedYear;

(ii) SeasonStartDate has a NonSpecifiedMonth;

(iii) the SeasonStartDate has a NonSpecifiedDayOfMonth;

then the S1SP shall, where it receives a Service Request that does not meet these criteria, create a SMETS1 Response indicating failure.

(s) Where the StandingChargeScale is different to the PriceScale (with their DUIS meanings) and the SMETS1 ESME does not correctly share that difference with HAN Devices then any HAN Device will incorrectly display the Standing Charge (with its SMETS1 meaning).

(t) Where the target SMETS1 ESME stores the Tariff Switching Table and the Non-Disablement Calendar (with their SMETS1 meanings) as one object whose capacity would be breached if the SwitchingTable (with its DUIS meaning) in the Service Request were to be stored, the S1SP shall create a SMETS1 Response indicating failure. This failure state may be resolved by resetting the Non-Disablement Calendar (with its SMETS1 meaning) as specified in clause 18.5(dd).

(u) Where a SpecifiedDayofWeek is not supported by the target SMETS1 GSME the S1SP shall set a NonSpecifiedDayOfWeek in all SeasonStartDates and SpecialDay elements, where either a SpecifiedDayOfWeek or a NonSpecifiedDayOfWeek (with their DUIS meanings) is specified in the Service Request.

(v) Not Used.

(w) Where, during the period of British Summer Time the target SMETS1 ESME is configured so that each StartTime (with its DUIS meaning) is one hour earlier than that specified in the Service Request, the switches between Tariff Registers (with its SMETS1 meaning) will be one hour earlier than specified in the Service Request.

(x) Where the PriceScale (with its DUIS meaning) is different to any configured Debt Recover Rates [1..2] scale (with its SMETS1 meaning) and the SMETS1 ESME does not correctly share that difference with HAN Devices, then any HAN Device will incorrectly display any of the Debt Recovery Rates [1..2] (with its SMETS1 meaning) where there is a difference.

(y) Where the PriceScale (with its DUIS meanings) is set to a value other than -5 and the SMETS1 ESME does not correctly share financial information with HAN Devices in such situations then, any HAN Device will incorrectly display Meter Balance, Time Debt Register[1...2], Payment Debt Register, Emergency Credit Balance, Emergency Credit Limit, Accumulated Debt and Emergency Credit Threshold (with their SMETS1 meanings).

(z) For such SMETS1 ESME, where:

(i) the Service Request only contains TOUPrices with an Index less than or equal to 15 then the S1SP shall set TOUPrice with Index 1 to 15, not specified in the TOUTariff (with their DUIS meanings), to zero in its instructions to the Device; or

(ii) the Service Request contains TOUPrices with an Index greater than 15 then the S1SP shall set TOUPrice with Index 1 to 48, not specified in the TOUTariff (with their DUIS meanings) to zero in its instructions to the Device and any HAN Device may incorrectly display any information.

(aa) Where the PriceScale (with its DUIS meanings) is set to a value other than -5 or the StandingCharge is set to a value other than -4 and the SMETS1 ESME does not correctly share financial information with HAN Devices in such situations then, any HAN Device will incorrectly display Meter Balance, Time Debt Register[1...2], Payment Debt Register, Emergency Credit Balance, Emergency Credit Limit, Accumulated Debt and Emergency Credit Threshold (with their SMETS1 meanings).

(bb) Where the target SMETS1 ESME does not accept non-zero Thresholds (with its DUIS meaning) when being configured to use Time-of-use Pricing (with its SMETS meaning); and

(i) The Thresholds (with its DUIS meaning) provided in the Service Request are non-zero, then the S1SP shall send a SMETS1 Response indicating failure; or

(ii) The Thresholds are not provided in the Service Request, then the S1SP shall configure the Device to apply zero to all Thresholds (with their DUIS meanings)

(cc) Where the target SMETS1 ESME does not support the setting of a tariff where:

(i) the SeasonStartDate has a NonSpecifiedMonth;

(ii) the SeasonStartDate has a NonSpecifiedDayofWeek;

(with their DUIS meanings) then the S1SP shall create a SMETS1 response indicating failure.

(dd) Where the target SMETS1 ESME does not support the setting of a tariff where any SpecialDays has a SpecifiedDayOfWeek then the S1SP will replace any SpecifiedDayOfWeek with a NonSpecifiedDayOfWeek when configuring the Device.

18.2 **Update Price (Primary Element) (SRV 1.2.1)**

(a) The provision of Clauses 18.1(a) to 18.1(j), 18.1(p), 18.1(q), 18.1(s) and 18.1(x) apply to this Service Request.

(b) Where the SMETS1 ESME or SMETS1 GSME does not reliably process instructions from an ‘Update Price (Primary Element)’ Service Request unless it has previously successfully processed instructions from an ‘Update Tariff (Primary Element)’ Service Request, the Device may, if no such prior ‘Update Tariff (Primary Element)’ Service Request has been processed, reject the Service Request leading to a SMETS1 Response indicating failure.

(c) For such SMETS1 ESME, where:

(i) the Service Request contains TOUPrices with an Index greater than 15 and the Device is currently configured with TOUPrices with Indices between 1 and 15, then the S1SP shall send a SMETS1 Response indicating failure; or

(ii) the Service Request contains TOUPrices with an Index less than or equal to 15 and the Device is currently configured with TOUPrices with Indices greater than 15, then the S1SP shall send a SMETS1 Response indicating failure.

18.3 Update Meter Balance (SRV 1.5)

(a) Where the target SMETS1 ESME or SMETS1 GSME does not support Adjust Meter Balance when Payment Mode is Credit Mode and the Device is in Credit Mode (with their SMETS meanings), the S1SP shall return a SMETS1 Response indicating failure.

(b) Where the target SMETS1 ESME or SMETS1 GSME has no function to ResetMeterBalance (with its DUIS meaning) in Credit Mode and the Payment Mode (with its SMETS1 meaning) is Credit and the Service Request specifies a ResetMeterBalance (with its DUIS meaning) the S1SP shall create a SMETS1 Response indicating failure.

(c) Where the target SMETS1 ESME or SMETS1 GSME may apply Payment based Debt Recovery (with its SMETS1 meaning) when a positive adjustment is made to the Meter Balance, the increase in the Meter Balance resulting from this Service Request may be correspondingly less than the adjustment specified.

(d) Where the target SMETS1 ESME or SMETS1 GSME does not support negative adjustments to the ESME Meter Balance/ GSME PrepaymentMode Meter Balance (with their DUIS and SMETS1 meanings) if the result of applying those adjustments would have been either to change the Meter Balance from a negative value to a more negative value or from a non-negative value to a negative value, then the S1SP shall create a SMETS1 Response indicating failure should such a Service Request be received.

(e) Where the target SMETS1 ESME or SMETS1 GSME processes a positive adjustment to the GSME PrepaymentMode Meter Balance (with their

DUIS and SMETS1 meanings) then the Device will, in addition to adjusting the Meter Balance (with its SMETS1 meaning), first apply that adjustment to the Accumulated Debt Register if it is greater than zero, second, if the accumulated Debt Register is zero, or is reduced to zero, apply any remaining adjustment to the Emergency Credit Balance until it reaches the Emergency Credit Limit.

(f) Where the SMETS1 GSME does not support the setting of Meter Balance (with its SMETS1 meaning) to greater than £20,000 then the S1SP shall, where it receives a Service Request that would result in a Meter Balance of greater than £20,000, return a SMETS1 Response indicating failure.

(g) The target SMETS1 ESME and SMETS1 GSME applies the adjustment in the following order:

(i) recovery of Payment-based Debt of an amount defined by Debt Recovery per Payment from the Payment Debt Register subject to the Debt Recovery Rate Cap;

(ii) recovery of debt accumulated in the Accumulated Debt Register;

(iii) increasing the meter balance until it reaches the non-disablement threshold;

(iv) repayment of Emergency Credit activated and used by Consumer; and

(v) adding remaining credit (the credit after deduction of i, ii, iii and iv above) to the Meter Balance.

(h) Where the target SMETS1 ESME does not support a zero value for AdjustMeterValue (with its DUIS meaning) then where such a Service Request is received, the S1SP shall create a SMETS1 Response indicating failure.

18.4 **<u>Update Payment Mode (SRV 1.6)</u>**

(a) When the S1SP changes Payment Mode (with its SMETS1 meaning) to Credit Mode, the SMETS1 ESME or SMETS1 GSME resets Meter Balance, Emergency Credit Balance, Emergency Credit Limit, Emergency Credit Threshold, Debt Recovery Rates [1 … 2] and Debt Recovery Per Payment (with their SMETS1 meanings).

(b) When the S1SP changes Payment Mode (with its SMETS1 meaning) to Prepayment, the SMETS1 ESME or GSME automatically activates Emergency Credit (with its SMETS1 meaning) if the Emergency Credit Limit (with its SMETS1 meaning) is greater than zero.

(c) When the S1SP changes Payment Mode (with its SMETS1 meaning) to Prepayment and no Emergency Credit Limit (with its SMETS1 meaning) has been set by way of a successful 'Update Prepayment Configuration (SRV 2.1)' more recently than the most recent Payment Mode (with its SMETS1 meaning) to change, an Emergency Credit Limit (with its SMETS1 meaning) of £5 shall apply on the Device.

(d) On a change of Payment Mode (with its SMETS1 meaning) the target SMETS1 ESME or SMETS1 GSME resets the Non-Disablement Calendar (with its SMETS1 meaning) to a factory default which is no Non-Disablement periods.

(e) Where the target SMETS1 ESME or SMETS1 GSME does not support positive values for the Disablement Threshold (with its SMETS1 meaning) and the DisablementThreshold value in the Service Request is positive (with their DUIS meanings), the S1SP shall create a SMETS1 Response indicating failure. For clarity, the S1SP shall undertake no further processing of the Service Request.

(f) Where the target SMETS1 ESME does not support the setting of the Disablement Threshold (with its SMETS1 meaning), the S1SP shall discard the value in DisablementThreshold when processing the Service Request. For clarity, the S1SP shall create a SMETS1 Response indicating success where all other processing succeeds and the SMETS1 ESME will continue to have the default Disablement Threshold (with its SMETS1 meaning) of zero.

(g) Where the target SMETS1 GSME does not support the setting of Suspend Debt Emergency (with its SMETS1 meaning) to be active and the value of SuspendDebtEmergency (with its DUIS meaning) is 'true' in the Service Request, the S1SP shall create a SMETS1 Response indicating failure. For clarity, the S1SP shall undertake no further processing of the Service Request.

(h) The S1SP shall read the Payment Mode (with its SMETS1 meaning) of the Device identified by the BusinessTargetID (with its DUIS meaning) and, where that is consistent with the PaymentMode (with its DUIS meaning), the S1SP shall create a SMETS1 Response indicating 'success', shall not send any instruction to the Device and shall ignore SuspendDebtEmergency, SuspendDebtDisabled and DisablementThreshold (with their DUIS meaning).

(i) Where the target SMETS1 GSME or SMETS1 ESME does not action the setting of Suspend Debt Disabled (with its SMETS1 meaning) to be active and the value of SuspendDebtDisabled (with its DUIS meaning) is 'true' in the Service Request, the S1SP shall configure the Device but the Device will continue with Time-based Debt Recovery.

(j) Where the target SMETS1 GSME or SMETS1 ESME does not collect Standing Charge when Suspend Debt Emergency (with its SMETS1 meaning) is active and the value of SuspendDebtEmergency (with its DUIS meaning) is 'true' in the Service Request, the S1SP shall configure the Device so that the Device does not collect Standing Charge.

(k) Where the SMETS1 ESME or the SMETS1 GSME supports the setting of DisablementThreshold (with its DUIS meaning) to a whole number of pence, the S1SP shall round up the value of DisablementThreshold (with its MMC meaning) to the nearest whole number of pence and instruct the device to apply the resulting value.

(l) When the S1SP changes Payment Mode (with its SMETS1 meaning) from Credit to Prepayment, the SMETS1 ESME or GSME will be configured with a NonDisablementCalendar (with its SMETS1 meaning) such that disablement of supply is suspended between 20:00 and 08:00 UTC on weekdays and all day on weekends.

(m) When the S1SP changes Payment Mode (with its SMETS1 meaning) from Credit to Prepayment, the SMETS1 ESME / GSME will reset the Meter Balance / PrepaymentMode Meter Balance (with its SMETS1 and DUIS meanings) respectively to zero.

(n) When the S1SP changes Payment Mode (with its SMETS1 meaning) from Credit to Prepayment, the SMETS1 ESME or GSME will be configured with an Emergency Credit Limit (with its SMETS1 meaning) of £10.

(o) When the S1SP changes Payment Mode (with its SMETS1 meaning) from Credit to Prepayment, the SMETS1 ESME or GSME will be configured with an Emergency Credit Threshold (with its SMETS1 meaning) of £1.

(p) When the S1SP changes Payment Mode (with its SMETS1 meaning) from Credit to Prepayment, the SMETS1 ESME or GSME will automatically activate Emergency Credit (with its SMETS1 meaning) if the Supply would have disabled due to insufficient credit.

(q) When the S1SP changes Payment Mode (with its SMETS1 meaning) from Credit to Prepayment, the SMETS1 ESME or GSME will be configured with a Maximum Meter Balance Threshold (with its SMETS2 meaning) of £1000.

(r) When the S1SP changes Payment Mode (with its SMETS1 meaning) from Credit to Prepayment, the SMETS1 ESME or GSME will be configured with a Maximum Credit Threshold (with its SMETS2 meaning) of £500.

(s) Where the target SMETS1 GSME or SMETS1 ESME does not suspend the collection of Time-based Debts (with its SMETS1 meaning) when SuspendDebtEmergency is set to true (with its DUIS meaning) then the Device shall, when Emergency Credit is activated (with its SMETS1 meaning) and SuspendDebtEmergency is set to true (with its DUIS meaning), collect any Time-based Debts from the Accumulated Debt Register (with their SMETS1 meanings).

(t) When setting Payment Mode to Prepayment Mode, regardless of whether the Device is currently in Credit Mode or Prepayment Mode, the target SMETS1 GSME:

(i) sets the Emergency Credit Balance to twice the Emergency Credit Limit and activates Emergency Credit, regardless of whether Emergency Credit is currently activated, or any Emergency Credit has been used thereby clearing any Emergency Credit that has been used (with their SMETS1 meanings). For clarity, any successful activation of Emergency Credit resulting from an Activate Emergency Credit (with its SMETS1 meanings) will set the Emergency Credit Balance to the Emergency Credit Limit; and

(ii) sets the Meter Balance, Payment Debt Register, Time Debt Registers [1 … 2] and the Accumulated Debt Register (with their SMETS1 meanings) to zero.

(u) Where the target SMETS1 GSME does not support positive values for the Disablement Threshold (with its SMETS1 meaning) and the DisablementThreshold value in the Service Request is positive (with their DUIS meanings), the S1SP shall create a SMETS1 Response indicating failure. For clarity, the S1SP shall undertake no further processing of the Service Request.

(v) When setting Payment Mode to Prepayment Mode, regardless of whether the Device is currently in Credit Mode or Prepayment Mode, the target

SMETS1 ESME:

(i) sets the Emergency Credit Limit to £5, or some other value that may have been set on the ESME prior to the ESME’s DateCommissioned (with its DUIS meaning), and sets the Emergency Credit Balance to twice that Emergency Credit Limit and activates Emergency Credit, regardless of whether Emergency Credit is currently activated, or any Emergency Credit has been used thereby clearing any Emergency Credit that has been used (with their SMETS1 meanings). For clarity, any successful activation of Emergency Credit resulting from an Activate Emergency Credit (with its SMETS1 meanings) will set the Emergency Credit Balance to the current Emergency Credit Limit; and

(ii) sets the Meter Balance, Payment Debt Register, Time Debt Registers [1 … 2] and the Accumulated Debt Register (with their SMETS1 meanings) to zero.

(w) When the S1SP changes Payment Mode (with its SMETS1 meaning) from Credit Mode to Prepayment Mode, the SMETS1 ESME or SMETS1 GSME resets the Accumulated Debt Register (with their SMETS1 meanings).

(x) When the S1SP changes Payment Mode (with its SMETS1 meaning) from Prepayment Mode to Prepayment Mode, the SMETS1 ESME does not reset the Accumulated Debt Register, the Emergency Credit Balance or the Meter Balance (with their SMETS1 meanings).

18.5 **Update Prepayment Configuration (SRV 2.1)**

(a) Where the target SMETS1 ESME or SMETS1 GSME does not support the update of Debt Recovery Rate Cap (with its SMETS1 meaning) when in Prepayment Mode (with its SMETS1 meaning) the S1SP shall ignore DebtRecoveryRateCap (with its DUIS meaning) if the Device is already in Prepayment Mode (with its SMETS1 meaning) and return a SMETS1 Response indicating success.

(b) Where the target SMETS1 ESME or SMETS1 GSME does not support the update of Debt Recovery Rate Cap (with its SMETS1 meaning) when in Credit Mode (with its SMETS1 meaning) the S1SP shall ignore DebtRecoveryRateCap (with its DUIS meaning) if the Device is in Credit Mode (with its SMETS1 meaning) and return a SMETS1 Response indicating success.

(c) Where the target SMETS1 ESME or SMETS1 GSME does not support the update of Low Credit Threshold (with its SMETS1 meaning) when in Prepayment Mode (with its SMETS1 meaning) the S1SP shall ignore LowCreditThreshold (with its DUIS meaning) if the Device is already in Prepayment Mode (with its SMETS1 meaning) and return a SMETS1 Response indicating success.

(d) Where the target SMETS1 ESME does not support StartDate and EndDate (with their DUIS meanings) for seasons and a StartDate (with its DUIS meaning) is specified that is in the future or an EndDate (with its DUIS meaning) is specified which is other than ‘3000-12-31T00:00:00Z’, the S1SP shall create a SMETS1 Response indicating failure.

(e) Where the target SMETS1 ESME does not support Special Days in a Non-Disablement Calendar (with their SMETS2 meanings) that do not specify all-day non-disablement and the Service Request specifies a SpecialDay (with its DUIS meaning) relating to a ElectricityNonDisablementSchedule (with its DUIS meaning) that has anything other than one SwitchTime (with its DUIS meaning) at midnight with a NonDisablementScript (with its DUIS meaning) set to START, the S1SP shall create a SMETS1 Response indicating failure.

(f) Where the target SMETS1 ESME only supports one Day Profile in a Non-Disablement Calendar (with its SMETS2 meaning) which has more than one period in it and the Service Request specifies an ElectricityNonDisablementSchedule (with its DUIS meaning) and DayOfWeekApplicability (with its DUIS meaning) that mandates more than one Day Profile that is set to not disable all day or has more than one period in it, the S1SP shall create a SMETS1 Response indicating failure.

(g) Where the target SMETS1 ESME or SMETS1 GSME does not have the capacity to store the Non-Disablement Calendar (with its SMETS meaning) requested, the S1SP shall create a SMETS1 Response indicating failure.

(h) For a target SMETS1 ESME or SMETS1 GSME, if the Service Request does not specify at least one NonDisablementScript with its DUIS meaning) that should apply on each day between the earliest StartDate and latest EndDate (with their DUIS meanings), the S1SP shall create a SMETS1 Response indicating failure.

(i) For a target SMETS1 GSME, if the Service Request does not specify at least one TimeStartAction (with its DUIS meaning) that should apply on each day after the earliest SeasonStartDate (with its DUIS meaning) as defined by the Service Request, the S1SP shall create a SMETS1 Response indicating failure.

(j) Where the target SMETS1 ESME does not support the equivalent of wildcards in the date in the ElecSpecialDayPrepayment fields (with its DUIS meaning) and the Service Request contains such wildcards, the S1SP shall create a SMETS1 Response indicating failure.

(k) Where the target SMETS1 GSME does not support the equivalent of wildcards in the SeasonStartDate fields or the date in the GasSpecialDayNonDisablement fields (with their DUIS meanings) and the Service Request contains such wildcards, the S1SP shall create a SMETS1 Response indicating failure.

(l) For a SMETS1 ESME that requires the check below to be successfully passed before it can process the instruction and the Service Request fails the check, the S1SP shall not action the Service Request and shall send a SMETS1 Response indicating failure. The check to be applied is:

1. Create an ordered list of all StartDates in the ElectricityNonDisablementCalendar

2. For each SpecialDayApplicability in each ElectricityNonDisablementSchedule, confirm that the date associated with that SpecialDayID (ignoring any years specified in that date) is:

   a) on or after the StartDate in that ElectricityNonDisablementSchedule (ignoring any years specified in that date) and

   b) is before the next subsequent StartDate (ignoring any years specified in that date) in the list created at step 1.

(m) Where the target SMETS1 ESME or SMETS1 GSME only supports setting of a MaxMeterBalance which is greater than the MaxCreditThreshold (with their DUIS meanings) the S1SP shall, where the Service Request does not meet these criteria, create a SMETS1 Response indicating failure.

(n) Where the target SMETS1 GSME only supports Debt Recovery Rate Cap (with its SMETS1 meaning) in whole numbers of pence, the S1SP shall round down the value in the DebtRecoveryRateCap (with its DUIS meaning), to the nearest whole pence and set the value of the Debt Recovery Rate Cap (with its SMETS1 meaning) to the value so calculated.

(o) Where the target SMETS1 ESME or the target SMETS1 GSME does not support this Service Request whilst operating in Credit Mode (with its SMETS1 meaning) and the Service Request is received whilst the device is operating in Credit Mode (with its SMETS1 meaning), the S1SP shall create a SMETS1 Response indicating failure.

(p) For SMETS1 ESME that can only support an ElectricityNonDisablementCalendar where:

(q) there are ElectricityNonDisablementSchedules, which in aggregate, are applicable to all seven days of the week;

(r) for every day covered by the ElectricityNonDisablementCalendar, there is an ElectricityNonDisablementSchedule with a ScheduleDatesAndTime where the time is midnight UTC; and

(s) in all days covered by the ElectricityNonDisablementCalendar there are at most three NonDisablementScripts that would apply during that day

(i) all SwitchTimes in ScheduleDatesAndTime of ElectricityNonDisablementSchedule are on the hour or half-hour.

(t) (with their DUIS meanings) and the Service Request does not meet all these criteria, the S1SP shall not action the Service Request and shall send a SMETS1 Response indicating failure.

(u) For SMETS1 ESME that do not support EndDates in ScheduleDatesAndTimes and do not support specified years in the StartDates of ScheduleDatesAndTimes, the S1SP shall instruct the ESME with a configuration where:

(i) the StartDate from each ScheduleDatesAndTime is treated as if there were a wildcard in the year of the StartDate; and

(ii) the EndDate in the Service Request is ignored, with the ESME treating the StartDate of each ScheduleDatesAndTime as ending the validity period of any ScheduleDatesAndTime with an earlier StartDate.

(v) Where the target SMETS1 ESME does not fully support StartDate and EndDate (with their DUIS meanings) and a StartDate (with its DUIS meaning) is specified where the year is other than ‘3000’ or an EndDate (with its DUIS meaning) is specified which is other than ‘3000-12-31’, the S1SP shall create a SMETS1 Response indicating failure.

(w) For SMETS1 ESME that can only support an ElectricityNonDisablementCalendar (with its DUIS meaning) where, in ElectricitySpecialDays, all SpecialDays, have a SpecifiedMonth, a SpecifiedDayOfMonth, and a NonSpecifiedDayOfWeek (with their DUIS meanings) and the Service Request does not meet this criteria, the S1SP shall not action the Service Request and shall send a SMETS1 Response indicating failure.

(x) For SMETS1 GSME that can only support a GasNonDisablementCalendar where:

(i) all StartTimes in all GasNonDisablementTimeStartActions are on the hour or half-hour;

(ii) the SeasonStartDate, has a NonSpecifiedYear, a SpecifiedMonth, a SpecifiedDayOfMonth and a NonSpecifiedDayOfWeek;

(iii) in all GasNonDisablementDayProfiles there are at most three NonDisablementAction elements;

(iv) all SpecialDays, have a SpecifiedMonth, a SpecifiedDayOfMonth and a NonSpecifiedDayOfWeek

(v) in each GasNonDisablementDayProfile there must be a GasNonDisablementTimeStartAction with a StartTime where the time is midnight UTC.

(with their DUIS meanings) and the Service Request does not meet all of these criteria, the S1SP shall not action the Service Request and shall send a SMETS1 Response indicating failure.

(y) Where the target SMETS1 ESME or SMETS1 GSME does not support a LowCreditThreshold which is less than the EmergencyCreditThreshold (with their DUIS meanings) then the S1SP shall create a SMETS1 Response indicating failure should such a Service Request be received.

(z) Where the target SMETS1 ESME or SMETS1 GSME does not support an EmergencyCreditThreshold when EmergencyCreditLimit is specified as zero, then the S1SP shall, where the EmergencyCreditLimit is zero, ignore the EmergencyCreditThreshold (with their DUIS meanings) but shall continue processing all other parts of the Service Request.

(aa) Where the target SMETS1 ESME or SMETS1 GSME only supports EmergencyCreditLimit, EmergencyCreditThreshold, LowCreditThreshold, MaxMeterBalance and MaxCreditThreshold (with their DUIS meanings) in whole numbers of pence, the S1SP shall round down all such values in the Service Request, to the nearest whole pence and configure the Device accordingly.

(bb) Where the target SMETS1 ESME does not support specified years in either StartDates or EndDates (with their DUIS meanings), the S1SP shall convert the year value in StartDate and EndDate as if they were wildcards and configure the Device accordingly.

(cc) Where the target SMETS1 ESME stores the Tariff Switching Table and the Non-Disablement Calendar (with their SMETS1 meanings) as one object whose capacity would be breached if the ElectricityNonDisablementCalendar (with its DUIS meaning) in the Service Request were to be stored, the S1SP shall create a SMETS1 Response indicating failure.

(dd) Where the target SMETS1 ESME stores the Tariff Switching Table and the Non-Disablement Calendar (with their SMETS1 meanings) as one object, merging failures with the Tariff Switching Table (with its SMETS1 meaning) may be resolved by submitting an Update Prepay Configuration Service Request with a single NonDisablementSchedule with:

(i) a NonDisablementScript with a value of “STOP”; and

(ii) a DayOf WeekID for all of:

(A) Monday

(B) Tuesday

(C) Wednesday

(D) Thursday

(E) Friday

(F) Saturday

(G) Sunday; and

(iii) a StartDate of 1st of January in any year and an EndDate of 31st of December in that same year; and

(iv) a SwitchTime of 00:00:00Z

(ee) Where the target SMETS1 GSME does not support different values for EmergencyCreditThreshold and LowCreditThreshold then the S1SP shall create a SMETS Response indicating failure should such a Service Request be received.

(ff) Where the target SMETS1 GSME does not support a DebtRecoveryRateCap (with its DUIS meaning) of greater than £99 per week, then the S1SP shall return a SMETS1 Response indicating failure should such a Service Request be received.

(gg) Where, during the period of British Summer Time the target SMETS1 ESME or SMETS1 GSME is configured so that each SwitchTime (with its DUIS meaning) is one hour earlier than that specified in the Service Request, the switches between periods in which Disablement of Supply is suspended (with its SMETS1 meaning) will be one hour earlier than specified in the Service Request.

(hh) The provisions of Clause 18.1(r) apply to this service request.

(ii) Not Used.

(jj) Where the target SMETS1 ESME successfully processes the Instructions arising from this Service Request, the Device will immediately create a BillingDataLog entry which would be returned as a result of a subsequent Retrieve Change Of Mode / Tariff Triggered Billing Data Log (SRV 4.4.2) Service Request which covers the period of this processing.

(kk) Not Used.

(ll) Subject to clause 18.5(bb), and where the target SMETS1 ESME receives a Service Request with an ElectricityNonDisablementSchedule with an

EndDate of 31st December 3000 then the Device will be configured to continue indefinitely from the StartDate (with their DUIS meanings).

(mm) Where the target SMETS1 GSME does not support any StartTimes (with their DUIS meaning) to a resolution of seconds then the SMETS1 GSME will ignore any seconds that are specified, and the Device will be configured with 00 seconds.

18.6 **Top Up Device (SRV 2.2)**

(a) The target SMETS1 ESME and SMETS1 GSME applies the credit added in the following order:

(i) recovery of Payment-based Debt of an amount defined by Debt Recovery per Payment from the Payment Debt Register subject to the Debt Recovery Rate Cap;

(ii) recovery of debt accumulated in the Accumulated Debt Register;

(iii) increasing the meter balance until it reaches the non-disablement threshold;

(iv) repayment of Emergency Credit activated and used by Consumer; and

(v) adding remaining credit (the credit after deduction of i, ii, iii and iv above) to the Meter Balance.

(b) Where the target SMETS1 ESME or SMETS1 GSME only supports UTRN values (with its DUIS meaning) that represent positive integer multiples of 100, then the S1SP shall, where the Command Variant is 2 or 3, return a SMETS1 Alert indicating failure, unless the UTRN value provided represents a positive integer multiple of 100. For clarity, DUIS states in section 1.4.7.5 that “For SMETS1 Service Requests with a Command Variant value of 2 or 3, the UTRN data item shall contain a 20 digit string (each digit taking a value of 0-9) representing value in pence, using leading zeros as necessary to give a 20 digit length.”

18.7 **Update Debt (SRV 2.3)**

(a) Where the target SMETS1 ESME or SMETS1 GSME only supports update of the recovery period for Debt Recovery Rates 1 and 2 (with their

SMETS1 meanings) when in Credit Mode (with its SMETS1 meaning) the S1SP shall ignore DebtRecoveryRatePeriod (with its DUIS meaning) if the Device is already in Prepayment Mode (with its SMETS1 meaning) and return a SMETS1 Response indicating success.

(b) Where the target SMETS1 ESME or SMETS1 GSME does not support the update of Debt Recovery Per Payment (with its SMETS1 meaning) when in Prepayment Mode (with its SMETS1 meaning) the S1SP shall ignore DebtRecoveryPerPayment (with its DUIS meaning) if the Device is already in Prepayment Mode (with its SMETS1 meaning) and return a SMETS1 Response indicating success.

(c) Where the target SMETS1 ESME or SMETS1 GSME only supports daily Debt Recovery Rates 1 and 2 (with their SMETS1 meanings) the S1SP shall ignore DebtRecoveryRatePeriod (with its DUIS meaning) if it has a value other than DAILY (with its DUIS meaning) and return a SMETS1 Response indicating success.

(d) Where the target SMETS1 ESME does not support Debt Recovery Rate 1 or 2 (with their SMETS1 meaning) with an accuracy of greater than hundred thousandths of Currency Units per day, the S1SP shall, where the Service Request specifies a DebtRecoveryRatePriceScale (with its DUIS meaning) of -6 or less, return a SMETS1 Response indicating failure.

(e) Where the target SMETS1 ESME does not support a Debt Recovery Rate 1 or 2 (with their SMETS1 meanings) at a resolution greater than ten thousandths of Currency Units per DebtRecoveryRatePeriod (with its DUIS meaning) and the DebtRecoveryRatePriceScale (with its DUIS meaning) specified is -5, the S1SP shall round the Debt Recovery Rate value (with its SMETS1 meaning) down to a whole number of ten thousandths of Currency Units (with its SMETS1 meaning) per DebtRecoveryRatePeriod (with its DUIS meaning).

(f) Where the target SMETS1 ESME or SMETS1 GSME only supports Debt Recovery per Payment (with its SMETS1 meaning) in whole numbers of percent, the S1SP shall divide the value in the DebtRecoveryPerPayment (with its DUIS meaning) by 100, round down to the nearest integer and set the value of the Debt Recovery per Payment (with its SMETS1 meaning) to the percentage so calculated.

(g) Where the target SMETS1 ESME or SMETS1 GSME does not support a DebtRecoveryRate (with its DUIS meaning) that is larger than 32767, the S1SP shall repeatedly divide the value of any such DebtRecoveryRate (with its DUIS meaning) by 10 and increase the associated scale by 1 until the resulting value can be stored on the device. The stored value shall be rounded down to the nearest integer if the value to store is no longer an integer after rescaling.

(h) Where the target SMETS1 ESME does not support a Time Debt Register 1 or 2 or Payment Debt Register (with their SMETS1 meanings) at a resolution greater than ten thousandths of Currency Units and given that the TimeDebtRegister1 or TimeDebtRegister2 or PaymentDebtRegister (with their DUIS meanings) are always specified at a resolution of hundreds of thousandths of Currency Units, the S1SP shall round the Time Debt Register 1 or 2 or Payment Debt Register value (with their SMETS1 meanings) down to a whole number of ten thousandths of Currency Units (with its SMETS1 meaning).

(i) Where the target SMETS1 ESME or SMETS1 GSME does not support setting of debt configuration when in Credit Mode (with its SMETS1 meaning) and the Device is in Credit Mode, the S1SP shall return a SMETS1 Response indicating failure.

(j) Where the target SMETS1 ESME does not support updating of debt values unless DebtRecoveryRatePriceScales are '-2', the S1SP shall, where the Service Request does not meet these criteria, return a SMETS1 Response indicating failure.

(k) Where the target SMETS1 ESME or SMETS1 GSME only supports daily Debt Recovery Rates 1 and 2 (with their SMETS1 meanings) and the DebtRecoveryRatePeriod (with its DUIS meaning) has a value other than DAILY (with its DUIS meaning), the S1SP shall return a SMETS1 Response indicating failure.

(l) Where the target SMETS1 ESME or SMETS1 GSME does not support a Time Debt Register 1 or 2 or Payment Debt Register (with their SMETS1 meanings) at a resolution greater than hundredths of Currency Units and given that the TimeDebtRegister1 or TimeDebtRegister2 or PaymentDebtRegister (with their DUIS meanings) are always specified at a resolution of hundreds of thousandths of Currency Units, the S1SP shall configure values which are the Time Debt Register 1 or 2 or Payment Debt Register value (with their SMETS1 meanings) the values specified, discarding the 3 least significant digits with the result being treated as a whole number of hundredths of Currency Units (with its SMETS1 meaning).

(m) Where the target SMETS1 GSME only supports Debt Recovery Rates (with their SMETS1 meaning) in whole numbers of pence, the S1SP shall round down the value in the DebtRecoveryRates (with their DUIS meaning), to the nearest whole pence and set the value of the Debt Recovery Rates (with its SMETS1 meaning) to the values so calculated.

(n) Where the target SMETS1 GSME requires that the DebtRecoveryRateCap (with its DUIS meaning) is set as part of this Service Request, and where the DebtRecoveryRateCap has not been previously set, then the S1SP shall set the DebtRecoveryRateCap to be £4.

(o) Where the target SMETS1 ESME successfully processes the Instructions arising from this Service Request, the Device will immediately create a BillingDataLog entry which would be returned as a result of a subsequent Retrieve Change Of Mode / Tariff Triggered Billing Data Log (SRV 4.4.2) Service Request which covers the period of this processing.

(p) Where any DebtRecoveryRatePriceScale (with its DUIS meaning) is different to the configured Tariff TOU Price Matrix / Tariff Block Price Matrix scale (with their SMETS1 meanings) and the SMETS1 ESME does not correctly share that difference with HAN Devices, then any HAN Device will incorrectly display any of the Debt Recovery Rates [1..2] where there is a difference (with its SMETS1 meaning).

(q) Whenever the S1SP processes this Service Request and any of the Debt Recovery Rates [1 … 2] or Debt Recovery per Payment (with their SMETS1 meanings) is set to 0, then SMETS1 GSME will not adjust the corresponding one of, or ones of, the Time Debt Register [1…2] or the Payment Debt Register (with their SMETS1 meanings) regardless of the contents of the SMETS1 Response.

18.8 <u>**Activate Emergency Credit (SRV 2.5)**</u>

(a) Where the SMETS1 ESME or SMETS1 GSME does not differentiate between the reasons for failure to activate Emergency Credit (with its SMETS1 meaning) then the S1SP shall return a SMETS1 Response indicating failure where the Device has indicated failure. This may indicate either that Emergency Credit (with its SMETS1 meaning) is not available for activation or is already activated.

(b) Where the SMETS1 ESME or SMETS1 GSME successfully actions the Instructions resulting from such a Service Request, the amount of Emergency Credit made available on the Device will be the Emergency Credit Limit less any amount that the Meter Balance is below the Disablement Threshold (with its SMETS1 meanings).

18.9 <u>Restrict Access for Change Of Tenancy(SRV 3.2)</u>

(a) Whenever the S1SP processes this Service Request and the meter Payment Mode (with its SMETS1 meaning) is Prepayment Mode, the SMETS1 ESME will set the Meter Balance and Emergency Credit Balance (with their SMETS1 meanings) operational data values to zero. The ESME will not invoke the current Emergency Credit Limit (with its SMETS1 meaning) and will go off supply unless the Non-Disablement Calendar (with its SMETS1 meaning) is configured to have a non-disablement period in force at the CoT time.

(b) Whenever the S1SP actions this Service Request and the meter Payment Mode (with its SMETS1 meaning) is Prepayment Mode, the SMETS1 GSME associated with the target SMETS1 GPF will set the Meter Balance and Emergency Credit Balance (with their SMETS1 meanings) operational data values to zero. The GSME will then invoke the current Emergency Credit Limit (with its SMETS1 meaning) to remain on supply.

(c) Not Used.

(d) Where the target SMETS1 ESME or SMETS1 GSME only restricts data from the date and time of execution of the command on the Device when, according to the Device’s clock, the RestrictionDateTime is in the past then the Device will ignore any RestrictionDateTime (with its DUIS meaning) configured in the Service Request and apply the restriction from the time of execution of the command.

(e) Where the provisions of clause 18.9(d) apply, the target SMETS1 ESME will also delete the data from the ProfileDataLog (with its SMETS1 meaning) on the device from the first data item in the log to the date and time that the restriction is applied.

18.10 <u>Clear Event Log (SRV 3.3)</u>

(a) Where the target SMETS1 ESME or SMETS1 GSME does not support the Clear Event Log command (with its SMETS1 meaning), the S1SP shall return a SMETS1 Response indicating failure and shall take no further action.

18.11 <u>Read Instantaneous Import Registers (SRV 4.1.1)</u>

This section intentionally left blank

18.12 Read Instantaneous Import TOU Matrices (SRV 4.1.2)

(a) Where it is not possible to retrieve all of the values from the target SMETS1 GSME then, in the SMETS1 Response, the values in TariffTOURegisterMatrixValue with indices 1 and 2 will be the values from the Device and the values with indices 3 and 4 will be 0 meaning that the values from the Device cannot be retrieved (with their MMC meanings).

18.13 Read Instantaneous Import TOU With Blocks Matrices (SRV 4.1.3)

(a) Where the SMETS1 ESME does not report values for the Tariff Block Counter Matrix (with their SMETS1 meaning), the values returned in CounterMatrixTOUValues (with their Message Mapping Catalogue meaning) in the SMETS1 Response shall all be zero.

(b) The provisions of Clause **Error! Reference source not found.** also apply to this Service Request.

18.14 Read Instantaneous Import Block Counters (SRV 4.1.4)

(a) Where the SMETS1 GSME reports tariff Block Counters (with their SMETS1 meaning) in kWh, the values returned ImportBlockCounters (with its Message Mapping Catalogue meaning) shall, contrary to Message Mapping Catalogue Section 5.20.2.2.2, be in units of kWh rather than meters cubed.

(b) Where the SMETS1 GSME does not report tariff Block Counters (with their SMETS1 meaning), the values returned in ImportBlockCounters (with its Message Mapping Catalogue meaning) in the SMETS1 Response shall all be zero.

(c) Where it is not possible to retrieve all of the values from the target SMETS1 GSME then, in the SMETS1 Response, the value in TariffBlockCounterValue with index 1 will be the value from the Device and the values with indices 2, 3 and 4 will be 0 meaning that the values from the Device cannot be retrieved (with their MMC meanings).

18.15 <u>Read Instantaneous Export Registers (SRV 4.2)</u>

This section intentionally left blank

18.16 <u>Read Instantaneous Prepay Values (SRV 4.3)</u>

(a) Where the SMETS1 GSME only supports reading of the value equivalent to PaymentDebtRegister (with its Message Mapping Catalogue meaning) to the nearest whole number of GBP , the value returned by the S1SP in the PaymentDebtRegister (with its Message Mapping Catalogue meaning) shall be the milli pence equivalent of the nearest whole number of GBP.

(b) Where the SMETS1 ESME or SMETS1 GSME has a value equivalent to DebtRecoveryRatePriceScale (with it DUIS meaning) greater than -5 and the SMETS1 Device returns the values equivalent to the TimeDebtRegister1and TimeDebtRegister2 (with their Message Mapping Catalogue meanings) to that scale , the values returned by the S1SP in the TimeDebtRegister1and TimeDebtRegister2 (with their Message Mapping Catalogue meanings) shall be rounded down so that they are accurate only to the scale specified in the DebtRecoveryRatePriceScale value.

(c) Where the target SMETS1 ESME or SMETS1 GSME does not support reading of Accumulated Debt Register, Emergency Credit Balance, Meter Balance, Payment Debt Register and the Time Debt Registers [1..2] (with their SMETS1 meanings) when the Payment Mode is Credit Mode and the Device is in Credit Mode (with their SMETS meanings), the S1SP shall return a SMETS1 Response indicating failure.

(d) Where the target SMETS1 ESME or SMETS1 GSME also records decreases in the Emergency Credit Balance and increases in the Accumulated Debt Register as decreases in the Meter Balance (with their SMETS1 meanings) then the corresponding values returned will reflect this behaviour.

18.17 <u>Retrieve Change Of Mode / Tariff Triggered Billing Data Log (SRV 4.4.2)</u>

(a) Where the target SMETS1 ESME or SMETS1 GSME does not support the recording of the values in the Tariff Block Counter Matrix when actioning a Set Payment Mode or Set Tariff command (with their SMETS meanings), the S1SP shall omit the TariffBlockCounterMatrix element in the SMETS1 Response (with its Message Mapping Catalogue meaning)**.**

(b) Where the SMETS1 GSME reports tariff Block Counters (with their SMETS1 meaning) in kWh, the values returned in BlockRegisterMatrixValue or TariffBlockCounterMatrix (with their Message Mapping Catalogue meanings) shall, contrary to Message Mapping Catalogue Sections , 5.23.2.2.4, 6.2.2.4 or 5.27.2.2 be in units of kWh rather than meters cubed.

(c) Where the SMETS1 ESME does not report values in these logs for the Tariff Block Counter Matrix (with its SMETS1 meaning), the S1SP shall create a SMETS1 Response with zero occurrences of TariffTOUBlock1RegisterMatrixValue TariffTOUBlock2RegisterMatrixValue TariffTOUBlock3RegisterMatrixValue and TariffTOUBlock4RegisterMatrixValue.

(d) Where the target SMETS1 ESME or SMETS1 GSME adds entries to the Billing Data Log (with its SMETS1 meaning) both before and after each triggering event, the SMETS1 Response shall contain details of both entries.

(e) Where it is not possible to retrieve all of the values from the target SMETS1 GSMEs log (with its SMETS1 meaning) then, in the SMETS1 Response:

(i) The values in TariffTOURegisterMatrixValue or TariffTOURegisterMatrix with indices 1 and 2 will be the values from the Device and the values with indices 3 and 4 will be 0 meaning that the values from the Device cannot be retrieved (with their MMC meanings); and

(ii) The value in BlockRegisterMatrixValue or BlockRegisterMatrix with index 1 will be the value from the Device and the values with indices 2, 3 and 4 will be 0 meaning that the values from the Device cannot be retrieved (with their MMC meanings).

(f) Where, pursuant to clause 18.42(e), the target SMETS1 GSME has stored additional LogEntries (with its MMC meaning), the SMETS1 Response shall contain details of these extra LogEntries where the period requested includes the corresponding timestamps.

(g) Where the time period specified in the Service Request should result in more than one LogEntry being returned from the target SMETS1 GSME, the S1SP shall return a single LogEntry that has a timestamp that is the first entry after the ReadLogPeriod StartDateTime (with their DUIS meanings).

(h) Where, pursuant to clauses 18.5(jj) and 18.7(o), the target SMETS1 ESME has stored additional LogEntries (with its MMC meaning), the SMETS1 Response shall contain details of these extra LogEntries where the period requested includes the corresponding timestamps.

(i) Where an Update Import Tariff (Primary Element) (SRV 1.1.1) or Update Payment Mode (SRV 1.6) Service Request has never been successfully executed in relation to the target SMETS1 ESME the S1SP shall return a SMETS1 Alert indicating failure.

(j) Where the target SMETS1 ESME does not reset block counters in accordance with the Billing Calendar timetable, the SMETS1 Response will contain Block Counters (with their SMETS1 meanings) that are always increasing in value and are never reset.

(k) Where the target SMETS1 ESME or SMETS1 GSME adds entries to the Billing Data Log (with its SMETS1 meaning) before the triggering event, the SMETS1 Response shall, where an Update Import Tariff (Primary Element) (SRV 1.1.1) has never been executed since the DateCommissioned (with its DUIS meaning), only contain details of consumption based on the tariff configuration that was configured before the Update Import Tariff (Primary Element) (SRV 1.1.1) was executed on the Device.

(l) Where the target SMETS1 ESME does not store any items within the Billing Data Log (with its SMETS1 meaning) when executing Update Price (Primary Element) (SRV 1.2.1), the SMETS1 Response shall not contain any LogEntries (with its MMC meaning) as a result of any execution of the Update Price (Primary Element) (SRV 1.2.1) Service Request.

(m) Where the target SMETS1 ESME supports a maximum of four or Eight Tariff Registers (with their SMETS1 meaning) then any SMETS1 Response will only contain consumption in either the first four or the first eight entries of the TariffTOURegisterMatrixValue (with its MMC meaning).

(n) Where the target SMETS1 ESME adds entries to the Billing Data Log (with its SMETS1 meaning) at midnight every day, the SMETS1 Response shall contain details of these extra LogEntries (with its MMC meaning) where the period requested includes the corresponding timestamps.

(o) Where the target SMETS1 GSME does not allow the reading of Operational data when performing an update to the Configuration data (with their SMETS1 meanings) then the SMETS1 response will return zero LogEntries (with its MMC meaning) where the device is still updating its Configuration data (with its SMETS1 meaning).

18.18 <u>Retrieve Billing Calendar Triggered Billing Data Log (SRV 4.4.3)</u>

(a) The provisions of Clauses 18.17 18.17(b) to 18.17(c) apply to this Service Request

(b) Where the target SMETS1 ESME or SMETS1 GSME may record such Billing Data Log (with its SMETS1 meaning) entries after midnight UTC even when the Billing Calendar (with its SMETS1 meaning) specifies midnight UTC then the SMETS1 Response may contain Timestamps (with their MMC meanings) reflecting the delayed recording.

(c) The provision of Clause 18.17 18.17(b) apply to this Service Request

(d) Where, pursuant to clause 18.42(e), the target SMETS1 GSME has stored LogEntries (with its MMC meaning) at different date-times than required by the Billing Calendar (with its SMETS1 meaning), the SMETS1 Response shall contain corresponding LogEntries.

(e) The provisions of Clause 18.17(g) apply to this Service Request.

(f) The provisions of Clause 18.21(e) apply to this Service Request.

(g) Where an Update Device Configuration (Billing Calendar) (SRV 6.8) Service Request has never been successfully executed in relation to the target SMETS1 ESME the S1SP shall return a SMETS1 Alert indicating failure.

(h) The provisions of Clause 18.17(j) also apply to this Service Request.

(i) The provisions of Clause 18.17(m) also apply to this Service Request.

(j) The provisions of Clause 18.17(n) also apply to this Service Request.

(k) The provisions of Clause 18.17(o) also apply to this Service Request.

(l) Where the SMETS1 ESME has, according to the EPCL, a GroupID = “EA” (with its EPCL meaning) then the SMETS1 Response shall not contain any LogEntries (with its MMC meaning) where the SMETS1 ESME has been configured with an ElectricityBillingCalendar Periodicity of Daily (with their DUIS meanings).

18.19 **Retrieve Billing Data Log (Payment Based Debt Payments) (SRV 4.4.4)**

(a) Where an Add Credit Command has never resulted in the recovery of any Payment-based Debt (with their SMETS1 meanings) on the target SMETS1 GSME the S1SP shall return a SMETS1 Alert indicating failure.

(b) Where the SMETS1 GSME does not share any Payment-based Debt (with its SMETS1 meaning) with the GPF on the same HAN then the S1SP shall return a SMETS1 Response that does not include any LogEntries (with its MMC meaning) derived from any Payment-based Debt collection.

18.20 **Retrieve Billing Data Log (Prepayment Credits) (SRV 4.4.5)**

(a) Where the LogEntry containing the PrepaymentCredits cannot be provided in the SMETS1 Response from the SMETS1 ESME, the S1SP shall, for each LogEntry, return an Unsupported Value for each PrepaymentCredits element in the SMETS1 Response (with their MMC meanings).

18.21 **Retrieve Import Daily Read Log (SRV 4.6.1)**

(a) The provisions of Clauses 18.17 18.17(b) to 18.17 18.17(c) apply to this Service Request

(b) Where the target SMETS1 ESME or SMETS1 GSME may record such Daily Read Log (with its SMETS1 meaning) entries after midnight UTC then the SMETS1 Response may contain Timestamps (with their MMC meanings) reflecting the delayed recording.

(c) Where the SMETS1 GSME takes snapshots at 23:00 UTC during the period of British Summer Time then any log entries for such periods will have such a corresponding 23:00 UTC timestamp.

(d) The provision of Clause 18.17(e) apply to this Service Request.

(e) Where the target SMETS1 GSME resets the TariffBlockCounterMatrix (with their Message Mapping Catalogue meaning) before taking a Billing Calendar (with its SMETS1 meaning) snapshot and this is the last day of the billing period then:

(i) Outside of British Summer Time the TariffBlockCounterMatrix values (with their MMC meaning) will all be 0; and

(ii) During British Summer Time the TariffBlockCounterMatrix will only reflect consumption for 23 of the 24 hours of the day.

(f) Where, pursuant to Clause 18.21(c), the time period specified in the Service Request includes the Timestamp of 00:00 of the current day and the current day is within BST and the Device processes the Service Request before 23:00 UTC, the target SMETS1 GSME will return a LogEntry with a Timestamp of 00:00 that will reflect the same consumption as recorded where the Timestamp is 23:00 (with their MMC meanings).

(g) The provisions of Clause 18.17(j) also apply to this Service Request.

(h) The provisions of Clause 18.17(m) also apply to this Service Request.

(i) The provisions of Clause 18.17(n) also apply to this Service Request.

(j) The provisions of Clause 18.17(o) also apply to this Service Request.

18.22 <u>Retrieve Active Import Profile Data (SRV 4.8.1)</u>

(a) Where the target SMETS1 GSME or SMETS1 GPF does not return any LogEntry (with its MMC meaning) where the StartDateTime is later than the DateCommissioned (with their DUIS meanings) of the target Device, then the S1SP shall return a Response without any LogEntry.

(b) Not Used.

(c) Not Used.

(d) Not Used.

(e) Pursuant to clause 18.9(d), where the target SMETS1 ESME, has deleted the data from the device, the only LogEntries (with its MMC meaning) returned in the SMETS1 Response will be those after the restriction has been applied unless there has been an active DSP Schedule for this service request that covers part of the ReadLogPeriod (with its DUIS meaning), in which case this data may be returned.

(f) Where the target SMETS1 GSME does not support the reading of more than 24 hours' worth of data and the ReadLogPeriod (with its DUIS meaning) is greater than 24 hours then the S1SP shall return a SMETS1 Response with 48 LogEntrys (with its MMC meaning) where the Timestamp of the first LogEntry (with their MMC meanings) will be equal to or later than the specified StartDateTime (with its DUIS meaning) in the request.

(g) The provisions of Clause 18.17(o) also apply to this Service Request.

18.23 <u>Read Reactive Import Profile Data (SRV 4.8.2)</u>

(a) Not Used.

(b) Not Used.

(c) Not Used.

(d) The provisions of clause 18.22(d) apply to this Service request.

(e) The provisions of Clause 18.17(o) also apply to this Service Request.

18.24 <u>Read Export Profile Data (SRV 4.8.3)</u>

(a) Not Used.

(b) Not Used.

(c) Not Used.

(d) The provisions of clause 18.22(d) apply to this Service request.

(e) The provisions of Clause 18.17(o) also apply to this Service Request.

18.25 Read Network Data (SRV 4.10)

(a) Where the target SMETS1 ESME does not support the Average RMS Over Voltage Counter or Average RMS Under Voltage Counter operational data items (with their SMETS meanings), the S1SP shall omit the AvgRMSOverVoltageCounter and AvgRMSUnderVoltageCounter elements in the SMETS1 Response (with its Message Mapping Catalogue meaning).

(b) Where the target SMETS1 GSME does not support the Network Data Log operational data item (with its SMETS meaning), the S1SP shall create a SMETS1 Response indicating failure.

(c) Where the target SMETS1 GSME requires an Instruction to begin logging in to the Network Data Log operational data item (with its SMETS meaning), the S1SP shall create a SMETS1 Response indicating failure, since the DCC do not support such Instructions.

(d) Where the target SMETS1 ESME does not support the Average RMS Voltage Profile Data Log (with its SMETS1 meaning) to have a period that is the same as the AverageRMSVoltageMeasurementPeriod (with its DUIS meaning) set for calculation of Average RMS Voltage (with its SMETS1 meaning) and the AverageRMSVoltageMeasurementPeriod has not been set to be the same as the Average RMS Voltage Profile Data Log period, the values returned in the Average RMS Voltage Profile Data Log shall be averages for the AverageRMSVoltageMeasurementPeriod calculated at the time of each log entry.

(e) Where the target SMETS1 ESME only supports the capture of voltages in the Average RMS Voltage Profile Data Log (with its SMETS1 meaning) with the same Average RMS Voltage Measurement Period (with its SMETS1 meaning), then any existing values, accessible via the

AvgRMSVoltageProfileDataLog (with its MMC meaning), will be erased whenever Average RMS Voltage Measurement Period (with its SMETS1 meaning) is changed from its previous value.

18.26 **Read Tariff (Primary Element) (SRV 4.11.1)**

(a) Where the target SMETS1 ESME does not support a StandingChargeScale (with its DUIS meaning) at a resolution greater than ten thousandths of Currency Units (with its SMETS1 meaning) per day the value in StandingChargeScale (with its Message Mapping Catalogue meaning) shall be -4 and the StandingCharge (with its Message Mapping Catalogue meaning) shall represent a value in a whole number of ten thousandths of Currency Units (with its SMETS1 meaning) per day.

(b) Where the target SMETS1 ESME does not support a PriceScale (with its DUIS meaning) at a resolution greater than ten thousandths of Currency Units (with its SMETS1 meaning) per kWh the value in PriceScale (with its Message Mapping Catalogue meaning) shall be -4 and the prices within the TariffTOUPriceMatrix and TariffBlockPriceMatrix (with their Message Mapping Catalogue meaning) shall represent values in a whole number of ten thousandths of Currency Units (with its SMETS1 meaning) per kWh.

(c) Where the SMETS1 ESME or SMETS1 GSME does not support StandingCharge (with its DUIS meaning) that is larger than 32767 the value in StandingChargeScale (with its Message Mapping Catalogue meaning) and the StandingCharge (with its Message Mapping Catalogue meaning) may be different to those previously requested, as defined in Clause 18.1(e).

(d) Where the SMETS1 ESME or SMETS1 GSME does not support prices in the TariffTOUPriceMatrix or TariffBlockPriceMatrix (with their DUIS meanings) that are larger than 32767 the value in PriceScale (with its Message Mapping Catalogue meaning) and the prices in TariffTOUPriceMatrix and TariffBlockPriceMatrix (with their DUIS meanings) may be different to those previously requested, as defined in Clause 18.1(f)

(e) Where the SMETS1 GSME does not support the setting of GasThresholdMatrix when TOUTariff (with their DUIS meanings) is present in a Update Import Tariff (Primary Element) Service Request, the S1SP shall not include a GasThresholdMatrix in a SMETS1 response where TOUTariff is present (with their MMC meanings).

(f) Where an Update Import Tariff (Primary Element) (SRV 1.1.1) Service Request has never been successfully executed in relation to the target SMETS1 GSME, or in relation to the SMETS1 GSME on the same home area network as the target SMETS1 GPF, the S1SP shall return a SMETS1 Response indicating failure.

(g) Where clause 18.1(dd) applies the SMETS1 response will only contain NonSpecifiedDayOfWeek for any configured SpecialDays (with their MMC meanings)

18.27 **Read Prepayment Configuration (SRV 4.13)**

(a) Where the target SMETS1 GSME does not support the Non-Disablement Calendar to be readable over the WAN Interface (with their SMETS meanings), the S1SP shall omit the NonDisablementCalendar element in the SMETS1 Response (with its Message Mapping Catalogue meaning).

(b) Where the value in DebtRecoveryRatePeriod (with its DUIS meaning) has previously been ignored pursuant to Clauses 18.7(c) and 18.7(e), the value of DebtRecoveryRatePeriod (with its Message Mapping catalogue meaning) in a SMETS1 response relating to an SMETS1 ESME shall correspondingly be unchanged.

(c) Where the value in DebtRecoveryRatePeriod (with its DUIS meaning) has previously been ignored pursuant to Clauses 18.7(c) and 18.7(e), the value of DebtRecoveryPeriod (with its Message Mapping catalogue meaning) in a SMETS1 response relating to a GSME shall correspondingly be unchanged.

(d) Where the target SMETS1 ESME does not support a Debt Recovery Rate 1 or 2 (with their SMETS1 meanings) at a resolution greater than ten thousandths of Currency Units per DebtRecoveryRatePeriod (with its DUIS meaning), the value in DebtRecoveryRatePriceScale (with its Message Mapping Catalogue meaning) shall be -4 and the DebtRecoveryRate (with its Message Mapping Catalogue meaning) shall be returned in a whole number of ten thousandths of Currency Units (with its SMETS1 meaning) per DebtRecoveryRatePeriod (with its DUIS meaning).

(e) Where the target SMETS1 ESME or SMETS1 GSME only supports Debt Recovery per Payment (with its SMETS1 meaning) in whole numbers of percent, the value in the DebtRecoveryPerPayment (with its Message Mapping Catalogue meaning) shall be a multiple of 100, where 100 represents one percent.

(f) Where the SMETS1 ESME or SMETS1 GSME does not support a DebtRecoveryRate (with its DUIS meaning) that is larger than 32767, the value in DebtRecoveryRatePriceScale (with its Message Mapping Catalogue meaning) and the DebtRecoveryRate (with its Message Mapping Catalogue meaning) may be different to those previously requested, as defined in Clause18.7(g).

(g) For the target SMETS1 ESME there may be additional ElectricityNonDisablementSchedule (with its Message Mapping Catalogue meaning) items that were not included in any prior 'Update Prepayment Configuration (SRV 2.1)' Service Request. Such additional items will have a switch time of midnight. These entries do not change the functional effect of the ElectricityNonDisablementCalendar (with its DUIS meaning).

(h) Where the target SMETS1 ESME stores a SuspendDebtDisabled and SuspendDebtEmergency (with their DUIS meanings) value for each debt type, the S1SP shall, in the SMETS1 response, populate SuspendDebtDisabled and SuspendDebtEmergency (with their Message Mapping Catalogue meanings) with the Device's Suspend Debt Disabled and Suspend Debt Emergency (with their SMETS1 meanings) values for Time Debt Register 1 (with its SMETS1 meaning). Additionally, if these values are not the same as the Suspend Debt Disabled and Suspend Debt Emergency (with their SMETS1 meanings) values for Time Debt Register 2 and Payment Debt Register (with their SMETS1 meanings), the S1SP shall send a S1SP Alert warning that the Suspend Debt settings are inconsistent.

(i) Where the SMETS1 ESME or SMETS1 GSME does not activate changes to prepayment configuration items until it switches to Prepayment Mode (with its SMETS1 meaning), the values returned by the Device for such items will not reflect any changes that are made whilst in Credit Mode (with its SMETS1 meaning). Therefore, the S1SP shall populate the SMETS1 Response in line with the Device provided information. For clarity, this applies to all data items that can be set in an 'Update Prepayment Configuration' Service Request except for ElectricityNonDisablementCalendar and GasNonDisablementCalendar (with their DUIS meanings).

(j) Where the SMETS1 GSME only supports the setting of DebtRecoveryRateCap (with its DUIS meaning) to a whole number of pence, the value of DebtRecoveryRateCap (with its MMC meaning) returned, shall be a whole number of pence.

(k) Where the target SMETS1 ESME or SMETS1 GSME does not support reading of Debt Recovery Per Payment, Debt Recovery Rate Cap, Disablement Threshold, Emergency Credit Limit, Emergency Credit Threshold, Low Credit Threshold, Suspend Debt Disabled, Suspend Debt Emergency, Non Disablement Calendar and Debt Recovery Rates[1..2] (with their SMETS1 meanings) when the Payment Mode is Credit Mode and the Device is in Credit Mode (with their SMETS meanings), the S1SP shall return a SMETS1 Response indicating failure.

(l) Where the SMETS1 GSME only supports the setting of DisablementThreshold (with its DUIS meaning) to a whole number of pence, the value of DisablementThreshold (with its MMC meaning) returned, shall be a whole number of pence.

(m) Where the clauses 18.7 (l) and 18.7 (m) apply, the DUIS values covered by those clauses which are returned in the SMETS1 Response, may be different from those previously requested.

(n) Where the target SMETS1 ESME or SMETS1 GSME only supports EmergencyCreditLimit, EmergencyCreditThreshold, LowCreditThreshold, MaxMeterBalance and MaxCreditThreshold (with its DUIS meaning) in whole numbers of pence, the values returned shall be in whole numbers of pence.

(o) For the target SMETS1 ESME, the S1SP will always return a year value of 5000 in all StartDates and EndDates (with their MMC meanings) and meaning that the Device is treating these values as wildcards.

(p) Where an Update Prepayment Configuration (SRV 2.1) Service Request has never been successfully executed in relation to the target SMETS1 GSME, or in relation to the SMETS1 GSME on the same home area network as the target SMETS1 GPF, the S1SP shall return a SMETS1 Response indicating failure..

(q) Where an Update Debt (SRV 2.3) Service Request has never been successfully executed in relation to the target SMETS1 GSME, the S1SP shall not return the DebtRecoveryRatePeriod element (with its MMC meaning) in the SMETS1 Response.

(r) Where Clause 18.5(ll) applies, the values returned for EndDates will reflect the day before the corresponding StartDates (with their DUIS meanings).

(s) Where the target SMETS1 ESME or SMETS1 GSME does not support the retrieval of the Disablement Threshold (with its SMETS1 meaning) and an Update Payment Mode (SRV 1.6) Service Request has never been successfully executed in relation to the target SMETS1 ESME or SMETS1 GSME, the S1SP shall return the relevant Unsupported Value for the Disablement Threshold value (with its SMETS1 meaning) in any SMETS1 Response.

(t) Where the SMETS1 ESME has never successfully processed a Set Payment Mode (with its DUIS meaning) Service Request and where the SMETS1 Response specifies SuspendDebtEmergency is true (with its MMC meaning) then this may not indicate that the GSME is behaving as required by SMETS1 in relation to Suspend Debt Emergency (with its SMETS1 meaning).

(u) Where clause **Error! Reference source not found.** applies, any StartTimes returned in the SMETS1 Response will always have 00 seconds.

18.28 <u>Read Load Limit Data (SRV 4.15)</u>

(a) Where the target SMETS1 ESME does not support Load Limit Power Threshold (with its SMETS1 meaning) at a resolution greater than 10s of Watts, the value in LoadLimitPowerThreshold (with its Message Mapping Catalogue meaning) shall have a value equating to a multiple of ten Watts.

18.29 <u>Read Active Power Import (SRV 4.16)</u>

This section intentionally left blank

18.30 <u>Read Meter Balance (SRV 4.18)</u>

(a) Where the target SMETS1 ESME or SMETS1 GSME does not support the Meter Balance to be accessible over the WAN Interface when Payment Mode is Credit Mode and the Device is in Credit Mode (with their SMETS meanings), the S1SP shall return a SMETS1 Response indicating failure.

18.31 **Read Device Configuration (Voltage) (SRV 6.2.1)**

(a) Where the target SMETS1 ESME does not support RMSExtremeUnderVoltageThreshold, RMSExtremeOverVoltageThreshold, AverageRMSOverVoltageThreshold, AverageRMSUnderVoltageThreshold, RMSVoltageSagThreshold and RMSVoltageSwellThreshold (with their SMETS1 meaning) at a resolution greater than one Volt, RMSExtremeUnderVoltageThreshold, RMSExtremeOverVoltageThreshold, AverageRMSOverVoltageThreshold, AverageRMSUnderVoltageThreshold, RMSVoltageSagThreshold and RMSVoltageSwellThreshold (with their Message Mapping Catalogue meaning) shall have values equating to whole number of volts.

(b) Where the target SMETS1 ESME only supports the setting of AverageRMSOverVoltageThreshold, AverageRMSUnderVoltageThreshold, RMSExtremeOverVoltageThreshold, RMSExtremeUnderVoltageThreshold, RMSVoltageSagThreshold and RMSVoltageSwellThreshold (with their DUIS Meanings) to a whole percentage of 230 volts, the S1SP shall return values for AverageRMSOverVoltageThreshold, AverageRMSUnderVoltageThreshold, RMSExtremeOverVoltageThreshold, RMSExtremeUnderVoltageThreshold, RMSVoltageSagThreshold and RMSVoltageSwellThreshold (with their MMC meanings) which are the values configured on the ESME rounded down to the nearest tenth of a volt.

18.32 **Read Device Configuration (Billing Calendar) (SRV 6.2.3)**

(a) Where the target SMETS1 ESME or SMETS1 GSME does not support a time other than midnight UTC in its Billing Calendar (with its SMETS1 meaning), the time values in BillingTime and BillingPeriodStart (with their Message Mapping Catalogue meanings) shall be midnight UTC.

(b) Where the target SMETS1 ESME or SMETS1 GSME does not support a time resolution greater than minutes in its Billing Calendar (with its SMETS1 meaning), the seconds values in BillingTime and BillingPeriodStart (with their Message Mapping Catalogue meanings) shall be zero.

(c) Where, pursuant to clause 18.42(e), the target SMETS1 ESME has stored a Billing Calendar (with its SMETS1 meaning) that is different to that specified in the prior ‘Update Device Configuration (Billing Calendar)’ (SRV 6.8) Service Request, the SMETS1 Response shall contain details of this different Billing Calendar.

(d) Where an Update Device Configuration (Billing Calendar) (SRV 6.8) Service Request has never been successfully executed in relation to the target SMETS1 GSME, or in relation to the SMETS1 GSME on the same home area network as the target SMETS1 GPF, the S1SP shall return a SMETS1 Response indicating failure.

(e) Where, pursuant to clause 18.42(e), the target SMETS1 GSME has stored a Billing Calendar (with its SMETS1 meaning) that is different to that specified in the prior 'Update Device Configuration (Billing Calendar)' (SRV 6.8) Service Request, the SMETS1 Response shall contain details of this different Billing Calendar.

18.33 <u>Read Device Configuration (Identity Exc MPxN) (SRV 6.2.4)</u>

(a) Where the target SMETS1 GSME does not support the Supply Tamper State or Supply Depletion State configuration data item (with their SMETS meanings), the S1SP shall omit the SupplyTamperState and SupplyDepletionState elements from the SMETS1 Response (with its Message Mapping Catalogue meaning).

(b) Where the SMETS1 ESME has never successfully processed a Set Electricity Supply Tamper State (SRV 6.25) or a or SMETS1 GSME has never successfully processed an Update Device Configuration (Gas Flow) (SRV 6.7) (with their DUIS meanings) Service Request and where the SMETS1 Response indicates SupplyTamperState is Unchanged (with its MMC meaning) then this may indicate that the SMETS1 ESME or SMETS1 GSME is behaving as required by SMETS1 in relation to SupplyTamperState (with its MMC meaning).

18.34 <u>Read Device Configuration (Instantaneous Power Thresholds) (SRV 6.2.5)</u>

(a) Where the target SMETS1 ESME does not support Low Medium Power Threshold and Medium High Power Threshold (with their SMETS1 meanings) at a resolution greater than tens of Watts, the value in LowMediumPowerThreshold and MediumHighPowerThreshold (with their Message Mapping Catalogue meanings) shall have values equating to a whole number of 10s of Watts.

18.35 **Read Device Configuration (Gas) (SRV 6.2.8)**

(a) Where the target SMETS1 GSME does not support the Uncontrolled Gas Flow Rate or the Conversion Factor configuration data items (with their SMETS meanings), the S1SP shall omit the UncontrolledGasFlowRate element or the ConversionFactor element (as the context requires) from the SMETS1 Response (with its Message Mapping Catalogue meaning).

(b) Where an Update Device Configuration (Gas Flow) (SRV 6.7) Service Request has never been successfully executed in relation to the target SMETS1 GSME, or in relation to the SMETS1 GSME on the same home area network as the target SMETS1 GPF, the S1SP shall return a SMETS1 Response indicating failure.

18.36 **Read Device Configuration (Payment Mode) (SRV 6.2.9)**

(a) Where the target SMETS1 GSME does not support the setting of Suspend Debt Emergency (with its SMETS1 meaning) to be active, the S1SP shall set the value of SuspendDebtEmergency (with its Message Mapping Catalogue meaning) to be ‘false’ in the SMETS1 Response.

(b) Where the target SMETS1 GSME does not support the reading of Suspend Debt Disabled (with its SMETS1 meaning), the S1SP shall omit the SuspendDebtDisabled (with its Message Mapping Catalogue meaning) from the SMETS1 Response.

(c) Where the SMETS1 GSME has never successfully processed a Set Payment Mode (with its DUIS meaning) Service Request and where the SMETS1 Response specifies SuspendDebtEmergency is true (with its MMC meaning) then this may not indicate that the GSME is behaving as required by SMETS1 in relation to Suspend Debt Emergency (with its SMETS1 meaning).

18.37 **Update Device Configuration (Load Limiting General Settings) (SRV 6.4.1)**

(a) Where the target SMETS1 ESME does not support Load Limit Power Threshold (with its SMETS1 meaning) at a resolution greater than tens of Watts, the S1SP shall divide the LoadLimitPowerThreshold (with its DUIS meaning) by 10, round down to the nearest whole number of tens of Watts and set the resulting value on the Device.

(b) Where the target SMETS1 ESME does not support Load Limit Power Threshold (with its SMETS1 meaning) at a resolution greater than Kilowatts, the S1SP shall divide the LoadLimitPowerThreshold (with its DUIS meaning) by 1000, round down to the nearest whole number of Kilowatts and set the resulting value on the Device.

(c) Where the target SMETS1 ESME does not support Load Limit Power Threshold (with its SMETS1 meaning) greater than 100,000 Watts, the S1SP shall, where the Service Request specifies a value greater than 100,000 Watts, return a SMETS1 Response indicating failure.

(d) Where the target SMETS1 ESME does not support a value of 'Unchanged' for LoadLimitSupplyState (with its DUIS meaning), then S1SP shall, where the Service Request specifies such a value, return a SMETS1 Response indicating failure.

(e) Where the target SMETS1 ESME does not support setting of the LoadLimitPeriod or the LoadLimitRestorationPeriod (with their DUIS meanings) the S1SP shall discard the values in LoadLimitPeriod and LoadLimitRestorationPeriod (with their DUIS meanings) when processing the Service Request. For clarity, the S1SP shall create a SMETS1 Response indicating success where all other processing succeeds.

18.38 <u>Update Device Configuration (Load Limiting Counter Reset) (SRV 6.4.2)</u>

(a) Where the SMETS1 ESME does not support the Reset Load Limit Counter command (with its SMETS1 meaning), the S1SP shall return a SMETS1 Response indicating failure.

18.39 <u>Update Device Configuration (Voltage) (SRV 6.5)</u>

(a) Where the target SMETS1 ESME does not support RMSExtremeUnderVoltageThreshold, RMSExtremeOverVoltageThreshold, AverageRMSOverVoltageThreshold, AverageRMSUnderVoltageThreshold, RMSVoltageSagThreshold and RMSVoltageSwellThreshold (with their SMETS1 meaning) at a resolution greater than one Volt, the S1SP shall divide the values in each of the RMSExtremeUnderVoltageThreshold, RMSExtremeOverVoltageThreshold, AverageRMSOverVoltageThreshold, AverageRMSUnderVoltageThreshold, RMSVoltageSagThreshold and RMSVoltageSwellThreshold (with their Message Mapping Catalogue meaning) by 10, round down to the nearest whole number of volts and set the resulting value on the Device.

(b) Where the target SMETS1 ESME only supports 60, 300, 600, 900, 1800 and 3600 for AverageRMSVoltageMeasurementPeriod (with its DUIS meaning), the S1SP shall set the value of Average RMS Voltage Measurement Period (with its SMETS1 meaning) to the next greater available measurement period if for AverageRMSVoltageMeasurementPeriod (with its DUIS meaning) is not equal to a supported value or, if the specified period is larger than 3600, set it to 3600.

(c) Where the target SMETS1 ESME only supports the setting of AverageRMSOverVoltageThreshold, AverageRMSUnderVoltageThreshold, RMSExtremeOverVoltageThreshold, RMSExtremeUnderVoltageThreshold, RMSVoltageSagThreshold and RMSVoltageSwellThreshold (with their DUIS meanings) to a whole percentage of 230v, then the S1SP shall round down the value in each of the AverageRMSOverVoltageThreshold, AverageRMSUnderVoltageThreshold, RMSExtremeOverVoltageThreshold, RMSExtremeUnderVoltageThreshold, RMSVoltageSagThreshold and RMSVoltageSwellThreshold (with their DUIS meanings) to the nearest whole percentage of 230v and configure the ESME accordingly.

(d) Where the target SMETS1 ESME successfully processes the Instructions resulting from this Service Request the device will erase the data used to populate the AvgRMSVoltageProfileDataLog (with its MMC meaning).

(e) Where the target SMETS1 ESME only supports 60, 120, 180, 240, 300, 360, 600, 720, 900, 1200 and 1800 for AverageRMSVoltageMeasurementPeriod (with its DUIS meaning), the S1SP shall set the value of Average RMS Voltage Measurement Period (with its SMETS1 meaning) to the next greater available measurement period if for AverageRMSVoltageMeasurementPeriod (with its DUIS meaning) is not equal to a supported value or, if the specified period is larger than 1800, set it to 1800.

(f) Where the target SMETS1 ESME only supports the setting of AverageRMSVoltageMeasurementPeriod (with its DUIS meaning) in multiples of 10 seconds, the S1SP shall round up the value in AverageRMSVoltageMeasurementPeriod to the next 10 second increment and configure the ESME accordingly.

(g) Where the target SMETS1 ESME supports the setting of AverageRMSOverVoltageThreshold, AverageRMSUnderVoltageThreshold and AverageRMSVoltageMeasurementPeriod (with their DUIS meanings) but does not ever trigger the event when these conditions are detected, then the S1SP will never send the relevant SMETS1 Alert (0x8F40 or 0x8F41).

18.40 **Update Device Configuration (Gas Conversion) (SRV 6.6)**

(a) Where the target SMETS1 GSME does not support the Conversion Factor configuration data item (with its SMETS meaning), the S1SP shall not set the Conversion Factor. For clarity, the S1SP shall create a SMETS1 Response indicating success where all other processing succeeds.

18.41 **Update Device Configuration (Gas Flow) (SRV 6.7)**

(a) Where the target SMETS1 GSME supports setting of the Uncontrolled Gas Flow Rate configuration data item (with its SMETS meaning) only to the range of values in Table 14, the S1SP shall set the Uncontrolled Gas Flow Rate (with its SMETS1 meaning) to the value that corresponds to the UncontrolledGasFlowRate (with its DUIS meaning) in Table 14.

UncontrolledGasFlowRate (with its DUIS meaning) (m3/hr)	Uncontrolled Gas Flow Rate (with its SMETS1 meaning) set on Device (m3/hr)
1	1.08
2	2.16
3 or greater	4.32

Table 14

(b) Where the target SMETS1 GSME does not support the Supply Tamper State, Uncontrolled Gas Flow Rate or Supply Depletion State configuration data items (with its SMETS meaning), the S1SP shall create a SMETS1 Response indicating failure.

(c) Where the target SMETS1 GSME does not support setting of the UncontrolledGasFlowRate, StabilisationPeriod or the MeasurementPeriod (with their DUIS meanings) the S1SP shall discard the values in UncontrolledGasFlowRate, StabilisationPeriod and MeasurementPeriod (with their DUIS meanings) when processing the Service Request. For clarity, the S1SP shall create a SMETS1 Response indicating success where all other processing succeeds.

18.42 Update Device Configuration (Billing Calendar) (SRV 6.8)

(a) Where the target SMETS1 ESME or SMETS1 GSME does not support a time other than midnight UTC in its Billing Calendar (with its SMETS1 meaning), the S1SP shall ignore the time elements of the BillingTime or BillingPeriodStart (with their DUIS meanings) and shall set the time in the Billing Calendar (with its SMETS1 meaning) to midnight UTC.

(b) Where the target SMETS1 ESME or SMETS1 GSME does not support a time resolution greater than minutes in its Billing Calendar (with its SMETS1 meaning), the S1SP shall ignore the seconds part of the time in the BillingTime or BillingPeriodStart (with their DUIS meanings) and shall set the seconds part of the time in the Billing Calendar (with its SMETS1 meaning) to zero.

(c) Where the target SMETS1 GSME does not support the Billing Calendar (with its SMETS1 meaning), the S1SP shall create a SMETS1 Response indicating failure.

(d) Where the target SMETS1 GSME only supports a Billing Calendar timetable of either (1) midnight daily, (2) weekly at midnight on Monday or (3) monthly at midnight on the first of the month (with its SMETS1 meaning) and the Service Request specifies a GasBillingCalendar (with its DUIS meaning) with a timetable that is other than one of those options, the S1SP shall create a SMETS1 Response indicating failure.

(e) Where the target SMETS1 ESME requires a Billing Calendar (with its SMETS1 meaning) with a start date in the past, and where a Periodicity of Yearly, SixMonthly or Quarterly (with their DUIS meanings) is specified in the Service Request, the S1SP shall derive, using the S1SP Time, a DayOf Month and BillingPeriodStartMonth (with their DUIS meanings) from the corresponding fields in the Service Request to ensure they refer to a dateTime (with its DUIS meaning) which is earlier than today, according to the S1SP Time.

(f) Where the SMETS1 GSME does not support BillingPeriodStart (with its DUIS meaning) in the future and the S1SP receives a Service Request where, according to the S1SPs current time, the BillingPeriodStart is in the future, then the S1SP shall return a SMETS1 Response indicating failure and undertake no further processing.

(g) Where the SMETS1 GSME does not support BillingPeriodStart (with its DUIS meaning) in the future and the S1SP receives a Service Request where, according to the S1SPs current time, the BillingPeriodStart is in the future, then the S1SP shall:

(i) derive, using the S1SP Time, a BillingPeriodStart by taking the specified BillingPeriodStart and decreasing it by the minimum number of periods specified in the Periodicity (with its DUIS meaning) in order to derive a date-time in the past; and

(ii) configure the Device with the resulting BillingPeriodStart, recognising that the time element will be ignored by the Device, in terms of when resulting Billing Data Log (with its SMETS1 meaning) entries are created. Rather the Device shall create such entries at 23:59:59 on the dates prior to the dates specified by the derived BillingPeriodStart and Periodicity. Additionally, the Device will immediately create a BillingDataLog entry which would be returned in a subsequent Retrieve Change Of Mode / Tariff Triggered Billing Data Log (SRV 4.4.2) Service Request which covers this period.

18.43 <u>Synchronise Clock (SRV 6.11)</u>

This section intentionally left blank

18.44 <u>Update Device Configuration (Instantaneous Power Threshold) (SRV 6.12)</u>

(a) Where the target SMETS1 ESME does not support Low Medium Power Threshold and Medium High Power Threshold (with their SMETS1 meanings) at a resolution greater than tens of Watts, the S1SP shall divide the LowMediumPowerThreshold and MediumHighPowerThreshold (with their DUIS meanings) by 10, round down to the nearest whole number of tens of Watts and set the resulting value on the Device.

18.45 <u>Read Event Or Security Log (SRV 6.13)</u>

(a) Where a LogEntry with a Timestamp (with their MMC meanings) that is earlier than the DateCommissioned (with its DUIS meanings) of the target SMETS1 ESME, SMETS1 GSME or SMETS1 CHF cannot be returned, then the S1SP shall, where the Service Request includes such a period, return a SMETS1 Response without any such LogEntry(s).

18.46 **Update Security Credentials (KRP) (SRV 6.15.1)**

This section intentionally left blank

18.47 **Request Handover of DCC Controlled Device (SRV 6.21)**

This section intentionally left blank

18.48 **Update Security Credentials (CoS) (SRV 6.23)**

This section intentionally left blank

18.49 **Retrieve Device Security Credentials (KRP) (SRV 6.24.1)**

This section intentionally left blank

18.50 **Set Electricity Supply Tamper State (SRV 6.25)**

This section intentionally left blank

18.51 **Update Device Configuration (RMS Voltage Counter Reset) (SRV 6.27)**

(a) Where the target SMETS1 ESME does not support the Average RMS Over Voltage Counter or Average RMS Under Voltage Counter operational data items (with their SMETS meanings), the S1SP shall create a SMETS1 Response indicating failure.

(b) Where the target SMETS1 ESME does not support the resetting of Average RMS Over Voltage Counter or Average RMS Under Voltage Counter operational data items (with their SMETS meanings), the S1SP shall create a SMETS1 Response indicating failure.

18.52 **Enable Supply (SRV 7.1)**

(a) Where the target SMETS1 ESME does not support the Enable Supply WAN Interface command (with its SMETS meaning), the S1SP shall create a SMETS1 Response indicating failure.

18.53 **Disable Supply (SRV 7.2)**

(a) Where the target SMETS1 ESME is in Prepayment Mode (with its SMETS1 meaning) and the Device has successfully executed the Instructions associated with the Service Request, the Device will automatically Arm Supply (with its DUIS meaning).

(b) Where the target SMETS1 GSME's Valve is Armed (with its SMETS1 meaning) then the S1SP shall create a SMETS1 response indicating failure.

18.54 **Arm Supply (SRV 7.3)**

This section intentionally left blank

18.55 **Read Supply Status (SRV 7.4)**

(a) Where the target SMETS1 GSME does not support the Remaining Battery Capacity to be capable of reading over the WAN Interface (with their SMETS meanings), the S1SP shall omit the RemainingBatteryCapacity element in the SMETS1 Response (with its Message Mapping Catalogue meaning).

18.56 **Commission Device (SRV 8.1.1)**

This section intentionally left blank

18.57 **Join Service (Critical) (SRV 8. 7.1)**

This section intentionally left blank

18.58 Join Service (Non-Critical) (SRV 8. 7.2)

This section intentionally left blank

18.59 Unjoin Service (Critical) (SRV 8. 8.1)

This section intentionally left blank

18.60 Unjoin Service (Non-Critical) (SRV 8. 8.2)

This section intentionally left blank

18.61 Read Device Log (SRV 8.9)

(a) For such SMETS1 CHF, any updates to the Device Log (with its SMETS1 meaning) will not be reflected in the SMETS1 Response for a period of up to two hours.

18.62 Update HAN Device Log (SRV 8.11)

(a) Where the SMETS1 CHF only supports a JoinTimePeriod (with its DUIS meaning) of up to 255 and the JoinTimePeriod (with its DUIS meaning) specified is greater than 255, the S1SP shall treat the JoinTimePeriod (with its DUIS meaning) as if it were 255.

(b) Where the SMETS1 CHF requires a Cyclic Redundancy Check (CRC) (with the meaning given by the ZigBee Alliance) to be present in the Install Code (with the meaning given by the ZigBee Alliance), the S1SP shall calculate the CRC from the InstallCode (with its DUIS meaning) and append to the InstallCode sending the resulting value to the Device.

(c) Where the RequestType (with its DUIS meaning) is Remove, and the target Device is a SMETS1 ESME, S1SP shall create a SMETS1 Response indicating failure and shall take no further action.

(d) Where the SMETS1 CHF only supports a JoinTimePeriod (with its DUIS meaning) in whole minutes then the S1SP shall round down the provided JoinTimePeriod (with its DUIS meaning) to the nearest whole number of minutes and instruct the Device accordingly.

(e) Where the SMETS1 CHF only supports a JoinTimePeriod (with its DUIS meaning) in whole minutes and the JoinTimePeriod (with its DUIS meaning) specified is less than 60 seconds, the S1SP shall return a SMETS1 Response indicating failure and take no further action.

(f) Not Used.

18.63 Update Firmware (SRV11.1)

(a) For any Device listed in this service request the S1SP shall not action the instruction in relation to that Device if an Activate Firmware Service Request for that Device is currently being processed. The DCC shall send an alert notifying the sender of the Service Request that the instruction has been discarded for the Device in question.

(b) Not Used.

(c) Where any Device listed in this Service Request is of a Device Model identified in Annex D, the S1SP shall send an Alert indicating failure.

(d) Where any Device listed in this Service Request is of a Device Model identified in Annex E, the resulting behaviours will be uncertain.

18.64 Read Firmware Version (SRV 11.2)

(a) Not Used.

(b) Where any Device listed in this Service Request is of a Device Model identified in Annex D, the S1SP shall send an Alert indicating failure.

(c) Where the target Device is of a Device Model identified in Annex F, the FirmwareVersion (with its MMC meaning) returned in the SMETS1 Response may not match the firmware_version held in the Central Products List.

18.65 **Activate Firmware (SRV 11.3)**

(a) Where more than 90 calendar days have elapsed since receipt by the DCC of the associated Update Firmware Service Request, the S1SP shall create a SMETS1 Response indicating failure and shall take no further action.

(b) Where a firmware upgrade process for the target Device or another Device on the same HAN is underway, the S1SP shall return a Response indicating failure.

(c) Not Used.

(d) Where a firmware upgrade process for the target Device or another Device on the same HAN is underway, the currently underway firmware upgrade process will be stopped and the S1SP shall return a SMETS1 Response indicating failure for the upgrade that has been stopped.

(e) Where any Device listed in this Service Request is of a Device Model identified in Annex E, the resulting behaviours will be uncertain.

19 S1SP recording of notified details

19.1 Whenever an S1SP has successfully authenticated a Service Request containing SupplierReplacementCertificates, or one containing ReplacementCertificates where the RemotePartyRole field has a value of Supplier (with their DUIS meaning), the S1SP shall, using the Certificates in SupplierReplacementCertificates or ReplacementCertificates (as the context requires), update the details it holds in relation to the target Device for each of:

(a) Notified Critical Supplier Certificate ID;

(b) Notified Non-Critical Supplier Certificate ID;

(c) Notified Critical Supplier ID; and

(d) Notified Non-Critical Supplier ID.

19.2 Whenever an S1SP has successfully authenticated a Service Request containing ReplacementCertificates where the RemotePartyRole field has a value of NetworkOperator (with their DUIS meaning), the S1SP shall, using the Certificates in ReplacementCertificates, update the details it holds in relation to the target Device for each of:

(a) Notified Critical Network Operator Certificate ID;

(b) Notified Non-Critical Network Operator Certificate ID;

(c) Notified Critical Network Operator ID; and

(d) Notified Non-Critical Network Operator ID.

20 Key rotation

20.1 As soon as reasonably practicable (and in any event within 7 days) following the Commissioning of a SMETS1 Communications Hub Function or a SMETS1 Smart Meter or a SMETS1 Gas Proxy Function or a SMETS1 PPMID, the S1SP shall, via the DCO, in relation to each such Device and where supported by that Device, re-generate and replace any Authentication Keys and any Encryption Keys (with their DLMS COSEM meanings) held by that Device.

21 Time

21.1 Where a Device is capable of maintaining time independently of any other Device within its SMETS1 Installation and where the S1SP is required to communicate with such a Device in order to process a SMETS1 Service Request and where the Device's time is within the DCC's set tolerance of S1SP Time, the S1SP shall synchronise the time on the Device with S1SP Time, and the DCO shall allow such synchronisation.

22 Anomaly Detection

22.1 Where an Anomaly Detection Threshold of the type referred to in (b)(ii) of the definition of Anomaly Detection Threshold has been set, the relevant DCO shall apply the relevant Threshold Anomaly Detection check immediately prior to returning any Instruction to the relevant SMETS1 Service Provider.

22.2 Where the Threshold Anomaly Detection check fails, the DCO shall not authorise any associated Instruction for the SMETS1 Device and shall respond to the relevant SMETS1 Service Provider accordingly. For the avoidance of doubt, the provisions of the Threshold Anomaly Detection Procedures that relate to the further processing of quarantined communications shall not apply to any consequentially deleted SMETS1 Service Requests and nor shall the DCC be required to notify the User of the deletion.

22.3 The DCC shall ensure that no Critical Instruction is sent to a SMETS1 Device unless the relevant DCO has confirmed that either:

(a) there is a Countersigned Service Request to which the Instruction appropriately corresponds; or

(b) the Instruction has been generated by the SMETS1 Service Provider in accordance with the provisions of Clause 20 or Clause 21 which apply to the Device Model of the relevant target Device.

22.4 In circumstances where a DCO is unable to confirm that an Instruction meets the requirements of Clause 22.3, the DCC shall:

(a) delete the Instruction from its systems;

(b) delete any related SMETS1 Service Request; and

(c) raise an Incident.

23 Additional S1SP Processing Values

23.1 Where the S1SP processing requires the additional data items laid out in in Annex C, the S1SP shall use the values laid out in Annex C for the Service Reference Variants specified in Annex C.

Annex A - Device Model Variations to Equivalent Steps Matrix (DMVES Matrix)

sec-appendix-am-an
nex-a-device-model-v

Annex B – Device Configuration Settings for Category 1 Devices

Configuration parameter where defined terms have their SMETS1 meaning	Values to be set where defined terms have their SMETS1 meaning
Sequence of debt recovery types	1- Payment-based Debt Recovery 2- Time-based Debt Recovery rates from the Debt Recovery Rates [1] 3- Time-based Debt Recovery rates from the Debt Recovery Rates [2]
Disablement of Supply not allowed	False
Recording period for the Profile Data Log	30 minutes
Recording period for the GSME Network Data Log	6 minutes
Stop collecting Standing Charge on Disablement of Supply due to insufficient credit	False
Load limiting measurement period	30 seconds
Future dated Commands	All such Commands must be cancelled
Maximum value of any price change command from a device on the same HAN	0
Average RMS Voltage Measurement Period	30 minutes

Table 15

Annex C – Default values for Service Requests for Category 1 Devices

SRV Affected	Default Parameter (with their SMETS1 meanings)	Value
1.6 2.1	Number of minutes to defer Disablement of Supply due to insufficient credit.	0
1.6 2.1	The maximum power that can be consumed when the Disablement Threshold has been breached and Emergency Credit is activated before the Supply is Disabled.	100kW
1.6 2.1	Number of minutes to defer Disablement of Supply due to expiration of the Non-Disablement Calendar and there being insufficient credit.	0
1.1.1 1.6 2.1	Payment Debt Registers, and Time Debt Register [1..2] will be reset on application.	False
1.6	Stop collecting Standing Charge when the Supply is Disabled due to insufficient credit	False
1.1.1 1.6	Trigger for the resetting of Block Counters	Billing Calendar

1.1.1 2.1	The time basis.	UTC
1.1.1	The default periodicity for resetting the Block Counters where no Billing Calendar has been set.	1 month
6.6	Publication of Gas Consumption data to the HAN	kWh and m^3

Table 16

Annex D – Firmware Exclusions

Any SMETS1 PPMID where:

- according to the EPCL, the GroupID = “DA” (with its EPCL meaning) and;
- the DeviceManufacturer is not “1031” (with its DUIS meaning).

Annex E – Firmware Exclusions

Any SMETS1 PPMID where:

- according to the EPCL, GroupID = “AA”, “BA”, “CA” or “CB” (with its EPCL meaning) or,
- according to the EPCL, the GroupID = “EA” (with its EPCL meaning) and the DeviceManufacturer is “1063” (with its DUIS meaning).

Annex F – Firmware Exclusions

Any SMETS1 PPMID where:

- according to the EPCL, the GroupID = “EA” or “EB” (with its EPCL meaning).

APPENDIX AN

SEC Variation Testing Approach Document for BEIS Changes included in the November 2020 SEC Release

[NOT IN USE]

Version 2.0

APPENDIX AO

S1SPKM COMPLIANCE POLICY

1 INTRODUCTION

1.1 The document comprising this Appendix AO:

a) shall be known as the "**S1SPKM Compliance Policy**" (and in this document is referred to simply as the "**Policy**"),
b) is a SEC Subsidiary Document required by Section L14.4(a)(v) of the Code (S1SPKI Assurance).

2 S1SPKI INDEPENDENT ASSURANCE SCHEME
DCC: Duty to Submit to an S1SPKI Independent Assurance Scheme

2.1 The DCC shall subject the S1SPKI Services to assessment against an assurance scheme which satisfies:

a) the quality requirements specified in Part 2.2 of this Policy;
b) the independence requirements specified in Part 2.3 of this Policy; and
c) the approval requirements specified in Part 2.5 of this Policy and that scheme is referred to in this Policy as the "**S1SPKI Independent Assurance Scheme**".

Quality Requirements

2.2 The quality requirements specified in this Part 2.2 are that the S1SPKI Independent Assurance Scheme must be a scheme:

a) which is recognised as an accreditation scheme for the purposes of Article 3(2) of Directive 1999/93/EC on a Community framework for electronic signatures;
b) which is based on ISO 27001; and
c) the provider of which:
(i) is used by the United Kingdom Government to provide assurance in relation to electronic trust services; and
(ii) requires all its scheme assessors to be UKAS certified.

Independence Requirements

2.3 The independence requirements specified in this Part 2.3 are that the provider of the S1SPKI Independent Assurance Scheme must be independent of the DCC and of each DCC Service Provider from which the DCC acquires capability for the purposes of the provision of the S1SPKI Services (referred to in this Policy as a "Relevant DCC Service Provider").

2.4 For the purposes of Part 2.3 of this Policy, the provider of the S1SPKI Independent Assurance Scheme is to be treated as independent of the DCC (and of Relevant DCC Service Providers) only if:
a) neither the DCC nor any of its subsidiaries (or any Relevant DCC Service Provider or any of its subsidiaries) holds or acquires any investment by way of shares, securities or other financial rights or interests in the provider of the scheme;
b) either:

(i) no director or employee of the DCC (or of any Relevant DCC Service Provider) is or becomes a director or employee of the provider of the scheme; or

(ii) where any person is or becomes both a director or employee of the DCC (or of any Relevant DCC Service Provider) and a director or employee of the provider of the scheme, appropriate arrangements are in place to ensure that that person is able to have no influence on any decisions made by the provider of the scheme in respect of the approval of any person or the accreditation of anything in accordance with the scheme;

c) no person who is a director or employee of the DCC (or of any Relevant DCC Service Provider) holds or acquires any investment by way of shares, securities or other financial rights or interests in the provider of the scheme, except where sub-paragraph (b)(ii) applies and that investment is acquired by that person by way of reasonable compensation for his or her performance as a director or employee of the provider of the scheme; and

d) the provider of the scheme does not hold or acquire a participating interest (as defined in section 421A of the Financial Services and Markets Act 2000) in the DCC (or in any Relevant DCC Service Provider).

Approval Requirements

2.5 Before entering into any agreement with the provider of the S1SPKM Independent Assurance Scheme, in accordance with its obligation under Section L15.2 of the Code (S1SPKM Compliance Policy), the DCC shall submit to the SMKI PMA for approval:

a) its proposed choice of scheme; and

b) the proposed terms and conditions of its agreement with the provider of that scheme,

and shall not enter into any such agreement unless the SMKI PMA has first approved the proposed S1SPKI Independent Assurance Scheme and the proposed terms and conditions of that agreement.

2.6 If the SMKI PMA does not approve either the proposed S1SPKI Independent Assurance Scheme or the proposed terms and conditions of the DCC's agreement with the provider of that scheme:

a) the SMKI PMA shall provide the DCC with a statement of its reasons for not doing so; and

b) the DCC shall submit to the SMKI PMA for approval, as soon as is reasonably practicable, a revised proposal in relation to the scheme.

3 INDEPENDENT ASSURANCE SERVICE PROVIDER

DCC: Duty to Procure Independent Assurance Services

3.1 For the purposes of complying with its obligation under Section L15.2 of the Code (S1SPKM Compliance Policy), the DCC shall procure the provision of assurance services:

a) of the scope specified in Part 3.2 of this Policy;

b) from a person who:

(i) is suitably qualified in accordance with Part 3.3 of this Policy; and

(ii) satisfies the independence requirements specified in Part 3.4 of this Policy,

and that person is referred to in this Policy as the “Independent S1SPKI Assurance Service Provider”.

Scope of Independent Assurance Services

3.2 The assurance services specified in this Part 3.2 are services in accordance with which the Independent S1SPKI Assurance Service Provider shall:

a) undertake an initial assessment of the S1SPKI Services against the S1SPKI Independent Assurance Scheme in accordance with Part 4 of this Policy;

b) subsequently undertake further assessments of the S1SPKI Services against the S1SPKI Independent Assurance Scheme:

(i) at a frequency recommended by the provider of that scheme; or

(ii) where there is no such recommended frequency, or where the SMKI PMA otherwise determines, at a frequency specified by the SMKI PMA;

c) at the request of, and to an extent determined by, the SMKI PMA, carry out an assessment of the compliance of any S1SPKI Participant with the applicable requirements of the S1SPKI Document Set;

d) at the request of the SMKI PMA, provide to it advice in relation to the compliance of any S1SPKI Participant with the applicable requirements of the S1SPKI Document Set;

e) at the request of the SMKI PMA, provide to it advice in relation to a review of this Policy, which shall include in particular:

(i) recommendations as to the scope and frequency of assessments carried out in accordance with this Policy; and

(ii) advice in relation to the suitability of any remedial action plan for the purposes of Section M8.4 of the Code (Consequences of an Event of Default), including where the Defaulting Party is the DCC in accordance with Section L15.6 of the Code (Events of Default); and

f) at the request of the SMKI PMA Chair, provide a representative to attend and contribute to the discussion at any meeting of the SMKI PMA.

Suitably Qualified Service Provider

3.3 The Independent S1SPKI Assurance Service Provider shall be treated as suitably qualified in accordance with this Part 3.3 only if it is recognised by the provider of the S1SPKI Independent Assurance Scheme as being qualified to carry out assessments against that scheme.

Independence Requirements

3.4 The independence requirements specified in this Part 3.4 are that the Independent S1SPKI Assurance Service Provider must be independent of each S1SPKI Participant and of each service provider from whom that S1SPKI Participant acquires capability for any purpose related to its compliance with its obligations under the Code (but excluding any provider of corporate assurance services to that S1SPKI Participant).

3.5 For the purposes of Part 3.4 of this Policy, the Independent S1SPKI Assurance Service Provider is to be treated as independent of an S1SPKI Participant (and of a relevant service provider of that S1SPKI Participant) only if:

a) neither that S1SPKI Participant nor any of its subsidiaries (or such a service provider or any of its subsidiaries) holds or acquires any investment by way of shares, securities or other financial rights or interests in the Independent S1SPKI Assurance Service Provider;

b) no director of that S1SPKI Participant (or of any such service provider) is or becomes a director or employee of, or holds or acquires any investment by way of shares, securities or other financial rights or interests in, the Independent S1SPKI Assurance Service Provider; and

c) the Independent S1SPKI Assurance Service Provider does not hold or acquire a participating interest (as defined in section 421A of the Financial Services and Markets Act 2000) in that S1SPKI Participant (or in any such service provider).

4 INITIAL ASSURANCE ASSESSMENT

DCC: Duty to Procure Initial Assessment

4.1 The DCC shall ensure that an initial assurance assessment of the S1SPKI Services:

a) against the S1SPKI Independent Assurance Scheme; and

b) in respect of compliance by the DCC with the applicable requirements of the S1SPKI Document Set,

is undertaken by the Independent S1SPKI Assurance Service Provider in accordance with Part 4.2 of this Policy.

Nature of the Initial Assessment

4.2 The initial assessment referred to in Part 4.1 of this Policy shall be undertaken by no later than such date as is necessary in order to ensure that an Assurance Report may be produced in relation to the S1SPKI Services being produced by the Independent SMKI Assurance Service Provider by no later than such date as the SMKI PMA shall determine to enable the SMKI PMA to make a recommendation relating to the Live Service Criteria relating to security for the relevant Eligible Product Combination List (EPCL).

4.3 The Assurance Report shall clearly identify any failure of the DCC to comply with any applicable requirements of the S1SPKI Document Set noting the severity of any non-compliances;

SMKI PMA: Response to the Initial Assessment

4.4 On receiving a S1SPKI Assurance Report, the SMKI PMA shall:

a) promptly consider that report;

b) determine that the assurance status of the DCC in relation to the S1SPKI Services is to be set at:

(i) approved;

(ii) approved with caveats; or

(iii) not approved;

c) where the SMKI PMA has set the assurance status of the DCC in relation to the S1SPKI Services at ‘approved with caveats’, state in writing its reasons for considering that it is acceptable for the DCC to commence the provision of the S1SPKI Services; and

d) provide a summary of any non-compliances and a SMKI PMA statement of its determination (and of any reasons accompanying that determination) to all Parties.

4.5 Where the SMKI PMA has set the assurance status of the DCC in relation to the S1SPKI Services at ‘approved with caveats’ or ‘not approved’ it shall:

a) require that the DCC submit to it as soon as reasonably practicable a remedial action plan; and

b) within one month of the submission of that plan, require the DCC to make any changes to it that the SMKI PMA may specify.

DCC: Duty in relation to Remedial Action Plan

4.6 Where the DCC is required to do so in accordance with Part 4.5(a) of this Policy, it shall as soon as reasonably practicable submit to the SMKI PMA a remedial action plan.

4.7 Where the DCC is required by the SMKI PMA in accordance with Part 4.5 of this Policy to make changes to the remedial action plan, it may appeal that decision to the SEC Panel and:

(a) the SEC Panel shall determine what changes (if any) shall be made to the remedial action plan; and

(b) the determination of the SEC Panel shall be final and binding for the purposes of the Code.

4.8 The DCC shall implement any remedial action plan subject to any required changes to it specified by:

a) the SMKI PMA in accordance with Part 4.5 of this Policy; or

b) the SEC Panel in accordance with Part 4.7 of this Policy.

5 Subsequent Assurance Assessments

5.1 Following the initial assessment, the DCC shall subsequently undertake further assessments of the S1SPKI Services against the S1SPKI Independent Assurance Scheme:

a) at a frequency recommended by the provider of that scheme;

b) where there is no such recommended frequency, or where the SMKI PMA otherwise determines, at a frequency specified by the SMKI PMA;

c) at the request of, and to an extent determined by, the SMKI PMA, carry out an assessment of the compliance of any S1SPKI Participant with the applicable requirements of the S1SPKI Document Set; or

d) at the request of the SMKI PMA, provide to it advice in relation to the compliance of any S1SPKI Participant with the applicable requirements of the S1SPKI Document Set.

5.2 On receiving a S1SPKI Assurance Report, the SMKI PMA shall:

a) promptly consider that report;

b) determine that the assurance status of the DCC in relation to the S1SPKI Services is to be set at:

(i) approved;

(ii) approved with caveats; or

(iii) not approved;

c) where the SMKI PMA has set the assurance status of the DCC in relation to the S1SPKI Services at ‘approved with caveats’, state in writing its reasons for considering that it is acceptable for the DCC to commence the provision of the S1SPKI Services; and

d) provide a summary of any non-compliances and a SMKI PMA statement of its determination (and of any reasons accompanying that determination) to all Parties.

5.3 Where the SMKI PMA has set the assurance status of the DCC in relation to the S1SPKI Services at 'approved with caveats' or 'not approved' it shall:

a) require that the DCC submit to it as soon as reasonably practicable a remedial action plan; and
b) within one month of the submission of that plan, require the DCC to make any changes to it that the SMKI PMA may specify.

5.4 Where the DCC is required by the SMKI PMA in accordance with Part 5.3 of this Policy to make changes to the remedial action plan, it may appeal that decision to the SEC Panel and:

a) the SEC Panel shall determine what changes (if any) shall be made to the remedial action plan; and
b) the determination of the SEC Panel shall be final and binding for the purposes of the Code.

5.5 The DCC shall implement any remedial action plan subject to any required changes to it specified by:

a) the SMKI PMA in accordance with Part 5.3 of this Policy; or
b) the SEC Panel in accordance with Part 5.4 of this Policy.

Version 2.0

Appendix AP1

S1SPKI Certificate Policy

Secure S1SP Certificate Policy for the Secure Cohort

Table of Contents

1 Introduction

The document comprising this Secure S1SP Certificate Policy (together with its Annexes A and B) shall be known as the "**Secure S1SP Certificate Policy**" (and in this document is referred to simply as the "**Policy**"). It is one of the S1SPKI Certificate Policies in the Smart Energy Code.

1.1 Overview

(A) This Policy sets out the arrangements relating to:

(i) SS1SP End Entity Certificates; and
(ii) SS1SPCA Certificates.

(B) This Policy is structured according to the guidelines provided by IETF RFC 3647, with appropriate extensions, modifications and deletions.

(C) Except where the context otherwise requires, words or expressions used in this Policy shall have the meanings ascribed to them in IETF RFC 5280 where they:

(i) appear in Courier New font;
(ii) are accompanied by the descriptor 'field', 'type' or 'extension'; and/or
(iii) take the form of a conjoined string of two or more words, such as 'digitalSignature'.

1.2 Document name and identification

(A) This Policy has not been assigned an OID.

1.3 Secure S1SP PKI (SS1SP PKI) participants

1.3.1 The Secure S1SP Certification Authority (SS1SPCA)

(A) The definition of Secure S1SP Certification Authority is set out in Annex A.

1.3.2 SS1SP PKI Registration Authorities

(A) The definition of SS1SP PKI Registration Authority is set out in Annex A.

1.3.3 Subscribers

(A) In accordance with the SS1SP PKI RAPP as set out in Annex E of this Policy, certain Parties may become Authorised Subscribers.

(B) In accordance with the SS1SP PKI RAPP as set out in Annex E of this Policy an Authorised Subscriber shall be an Eligible Subscriber in relation to certain Certificates.

(C) The SS1SP PKI RAPP as set out in Annex E of this Policy sets out the procedure to be followed by an Eligible Subscriber in order to become a Subscriber for one or more Certificates.

(D) Eligible Subscribers are subject to the applicable requirements of the SS1SP PKI RAPP as set out in Annex E of this Policy and Subscriber Obligations as set out in Annex C this Policy.

(E) Obligations on the Secure S1SP acting in the capacity of an Eligible Subscriber can be found in the SS1SP PKI RAPP as set out in Annex E of this Policy.

(F) The definitions of the following terms are set out in Annex A of this Policy:

(i) Authorised Subscriber;

(ii) Eligible Subscriber;

(iii) Subscriber.

1.3.4 Subjects

(A) The Subject of a SS1SP End Entity Certificate is represented by an appropriate identifier in the subject field of the SS1SP End Entity Certificate Profile (as the case may be) in accordance with Annex B.

(B) The Subject of a SS1SPCA Certificate must be the entity identified by the subject field of the Root SS1SPCA Certificate Profile, the Intermediate SS1SPCA Certificate Profile or the Subordinate SS1SPCA Certificate Profile (as the case may be) in accordance with Annex B.

(C) The definition of Subject is set out in Annex A.

1.3.5 Relying Parties

(A) In accordance with this Policy, certain Parties may be Relying Parties.

(B) Relying Parties are subject to the applicable requirements of the Relying Party Obligations as set out in Annex D of this Policy.

(C) Obligations on the Secure S1SP acting in the capacity of a Relying Party are set out in Annex D: Relying Party Obligations of this Policy.

(D) The definition of Relying Party is set out in Annex A.

1.3.6 SS1SP PKI Policy Management Authority

(A) The duties of the SS1SP PKI Policy Management Authority fall under the Security Sub-Committee for PKI (SSC for PKI). This executive group is responsible for fulfilling the duties of the PMA in relation to the SS1SP PKI. The terms of reference for operation of SSC for PKI is outlined in SSC for PKI Terms of Reference _1.0

1.3.7 SS1SP PKI Repository Provider

(A) SS1SPCA will be the SS1SP PKI Repository Provider.

1.4 Usage of SS1SP end entity certificates and SS1SPCA certificates

1.4.1 Appropriate Certificate Uses

(A) The Subordinate SS1SPCA shall ensure that SS1SP End Entity Certificates are Issued only:

(i) to Eligible Subscribers; and

(ii) for the purposes of:

a) the creation, sending, receipt and processing of communications to and from Secure SMETS1 Devices in accordance with or pursuant to the Smart Energy Code (SEC), which will further include:

1) Symmetric key generation (Digital Signature, Key Agreement);

2) Code signing (Digital Signature, Non-Repudiation, Code Signing);

3) TLS Communication (Digital Signature, Key Agreement, TLS Web Client Authentication, TLS Web Server Authentication); and

4) Authentication and Non-Repudiation of Secure SMETS1 Devices (Digital Signature, Non Repudiation, Key Encipherment, Data Encipherment, Key Agreement, TLS

Web Client Authentication, TLS Web Server Authentication).

(B) The SS1SPCA shall ensure that SS1SPCA Certificates are Issued only to the SS1SPCA:

(i) in its capacity as, and for the purposes of exercising the functions of, the Root SS1SPCA;

(ii) in its capacity as, and for the purposes of exercising the functions of, the Intermediate SS1SPCA; and

(iii) in its capacity as, and for the purposes of exercising the functions of, the Subordinate SS1SPCA.

(C) Further provision in relation to the use of Certificates is made in the Subscriber Obligations as set out in Annex C of this Policy and the Relying Party Obligations as set out in Annex D of this Policy.

1.4.2 Prohibited Certificate Uses

(A) No Party shall use a Certificate other than for the purposes specified in Part 1.4.1 of this Policy.

1.5 Policy administration

1.5.1 Organisation administering the Document

(A) This Policy is a Secure S1SP document and is administered as such in accordance with the provisions of this Policy and any supporting Policy documents.

1.5.2 Contact Person

(A) Questions in relation to the content of this Policy should be addressed to the Secure S1SP's CISO (Chief Information Security Officer).

1.5.3 Person determining SS1SP CPS suitability for the Policy

(A) Security subcommittee for PKI (SSCPKI) will be responsible for determining the suitability of the SS1SP CPS.

1.5.4 SS1SP CPS approval procedures

(A) The SSCPKI shall approve the SS1SP CPS.

(B) The SS1SP shall keep the SS1SP CPS under review and shall in particular carry out a review of the SS1SP CPS whenever (and to the extent to which) it may be required to do so by the Security Sub committee for PKI

(C) Following any review of the SS1SP CPS:

(i) the SS1SP may propose amendments to it, which it shall submit to the SSCPKI for its approval; and

(ii) those amendments may be made only to the extent to which the SSCPKI has approved them.

1.5.5 Registration Authority Policies and Procedures

(A) The SS1SP PKI Registration Authority Policies and Procedures (the SS1SP PKI RAPP are set out in in Annex E of this Policy.

1.6 Definitions and acronyms

1.6.1 Definitions

(A) Definitions of the expressions used in this Policy are set out in Annex A and shall otherwise be interpreted in accordance with the Smart Energy Code.

1.6.2 Acronyms

(A) Any acronyms used for the purposes of this Policy are set out in Annex A.

2 Publication and repository responsibilities

2.1 Repositories

2.2 SS1SP PKI Repositories

(A) Each SS1SPCA has its own secure, encrypted repository that contains:

(i) Its private key (held in encrypted state at rest and subject to Secret Shares - see Parts 6.2.2 and 6.2.4 of the SS1SP CPS);

(ii) Copies of all Certificates generated and issued; and

(iii) Audit Log information with regards to the SS1SPCA functions which includes:

a) Certificate issued

b) Certificate date and time of issuance

c) Other data and data sets related to Certificates e.g. CSR.

2.3 Publication of certification information

(A) See Part 2.2 of the Policy.

2.4 Time or frequency of publication

(A) Immediately upon a Certificate being generated and issued by the SS1SPCA.

2.5 ACCESS CONTROLS ON SS1SP PKI REPOSITORIES

(A) All SS1SP PKI Repositories are subject to stringent access controls. Only authorised SS1SPCA Systems and Privileged Users have access to SS1SP PKI Repositories.

(B) All SS1SP PKI Repositories are:

(i) Encrypted using AES-128 (Galois Counter Mode);

(ii) Held off-line and not network connected until required; and

(iii) Reside in data centres in accordance with Part 5 of this Policy.

(C) SS1SPCA Private Keys held within the SS1SP PKI Repository are encrypted and further secured using M of N Secret Shares as described in Part 6.2.2 of this Policy.

3 Identification and authentication

3.1 Naming

3.1.1 Types of Names

(A) The SS1SPCA will ensure that the name of the Subject of each Certificate is in accordance with the relevant Certificate Profile at Annex B.

3.1.2 Need for Names to be Meaningful

(A) The SS1SPCA will ensure that the name of the Subject of each Certificate is meaningful and consistent with the relevant Certificate Profile in Annex B.

3.1.3 Anonymity or Pseudonymity of Subscribers

(A) Under this Policy, the SS1SPCA will:

(i) prohibit Eligible Subscribers from requesting the Issue of a Certificate anonymously or by means of a pseudonym.

3.1.4 Rules for Interpreting Various Name Forms

(A) Provision in relation to name forms is made in Annex B.

3.1.5 Uniqueness of Names

(A) Provision in relation to the uniqueness of names is made in Annex B.

3.1.6 Recognition, Authentication, and Role of Trademarks

(A) No Eligible Subscriber may make a Certificate Signing Request which contains:

(i) any information that constitutes a trademark, unless it is the holder of the Intellectual Property Rights in relation to that trade mark; or

(ii) any confidential information which would be contained in a Certificate Issued in response to that Certificate Signing Request.

3.2 Initial identity verification

3.2.1 Method to Prove Possession of Private Key

(A) Provision is made in the SS1SP PKI RAPP as set out in Annex E of this Policy in relation to:

(i) the procedure to be followed by an Eligible Subscriber in order to prove its possession of the Private Key which is associated with the Public Key to be contained in any Certificate that is the subject of a Certificate Signing Request; and

(ii) the procedure established for this purpose is in accordance with the procedure in PKCS#10 or an equivalent cryptographic mechanism.

3.2.2 Authentication of Organisation Identity

(A) Only the Secure S1SP organisation is allowed to subscribe for Certificates under this Policy.

3.2.3 Authentication of SS1SP Parties

(A) Provision is made in the SS1SP PKI RAPP as set out in Annex E of this Policy in relation to the Authentication of SS1SP Parties engaged as Authorised Subscribers, which provides for all such persons to have their identity and authorisation verified against a robust and assured authentication framework as agreed by the SSC for PKI.

3.2.4 Non-verified Subscriber Information

(A) The SS1SPCA shall:

(i) verify all information in relation to SS1SPCA Certificates;

(ii) require each Eligible Subscriber to verify the information contained in any Certificate Signing Request in respect of a SS1SP End Entity Certificate.

(B) Further provision on the content of SS1SPCA Certificates is made in Subscriber Obligations as set out in Annex C of this Policy.

3.2.5 Validation of Authority

(A) See Part 3.2.2 of this Policy.

3.2.6 Criteria for Interoperation

(A) [Not applicable in this Policy]

3.3 Identification and authentication for re-key requests

3.3.1 Identification and Authentication for Routine Re-Key

(A) This Policy only supports a limited Certificate Re-Key service.

(B) The SS1SPCA shall provide a Certificate Re-Key service for SS1SPCA End Entity Certificates with the SMSO TLS Certificate profile and the SMSO KMS Certificate Profile as defined in Annex B.

(C) SS1SPCA End Entity Certificates with the Certificate Profiles in (B) above will be re-keyed every 5 years.

(D) Identification and authentication for routine re-key will be as per Part 3.2 of this Policy.

3.3.2 Identification and Authentication for Re-Key after Revocation

(A) [Not applicable in this Policy]

3.4 Identification and authentication for revocation request

(A) [Not applicable in this Policy]

4 Certificate life-cycle operational requirements

4.1 Certificate application

4.1.1 Submission of Certificate Applications

(A) Provision is made in the SS1SP PKI RAPP as set out in Annex E of this Policy in relation to:

(i) in respect of a SS1SP End Entity Certificate:

a) the circumstances in which an Eligible Subscriber may submit a Certificate Signing Request; and

b) the means by which it may do so, including through the use of an authorised System; and

(ii) in respect of a SS1SPCA Certificate, the procedure to be followed by an Eligible Subscriber in order to obtain a SS1SPCA Certificate.

4.1.2 Enrolment Process and Responsibilities

(A) Provision is made where applicable in the SS1SP PKI RAPP as set out in Annex E of this Policy in relation to the:

(i) establishment of an enrolment process in respect of organisations, individuals, Systems and Secure SMETS1 Devices in order to Authenticate them and verify that they are authorised to act on behalf of an Eligible Subscriber or Authorised Subscriber in its capacity as such; and

(ii) maintenance by the SS1SPCA of a list of organisations, individuals, Systems and Secure SMETS1 Devices enrolled in accordance with that process.

4.1.3 Enrolment Process for the Registration Authority and its Representatives

(A) Provision is made in the SS1SP PKI RAPP as set out in Annex E of this Policy in relation to the establishment of an enrolment process in respect of SS1SPCA Personnel and SS1SPCA Systems:

(i) in order to Authenticate them and verify that they are authorised to act on behalf of the SS1SPCA in its capacity as the Registration Authority; and

(ii) including in particular, for that purpose, provision:

(a) for Authentication of all Registration Authority Personnel by a Registration Authority Manager; and

(b) for all Registration Authority Personnel to have their identify and authorisation verified against a robust assured authentication framework as agreed by the SSC for PKI.

4.2 Certificate application processing

4.2.1 Performing Identification and Authentication Functions

(A) Provision is made in the SS1SP PKI RAPP as set out in Annex E of this Policy in relation to the Authentication by the SS1SPCA of Eligible Subscribers which submit a Certificate Signing Request.

4.2.2 Approval or Rejection of Certificate Applications

(A) Where any Certificate Signing Request fails to satisfy the requirements set out in the SS1SP PKI RAPP as set out in Annex E of this Policy or this Policy, the SS1SPCA:

(i) shall reject it and refuse to Issue the Certificate which was the subject of the Certificate Signing Request; and

(ii) may give notice to the Party which made the Certificate Signing Request of the reasons for its rejection.

(B) Where any Certificate Signing Request satisfies the requirements set out in the SS1SP PKI RAPP as set out in Annex E of this Policy or any other provision of this Policy, the SS1SPCA shall Issue the Certificate which was the subject of the Certificate Signing Request.

4.2.3 Time to Process Certificate Applications

(A) All Certificate applications to the SS1SPCA will be processed within 7 days.

4.3 Certificate issuance

4.3.1 SS1SPCA Actions during Certificate Issuance

(A) The SS1SPCA may Issue a Certificate only:

(i) in accordance with the provisions of this Policy and the SS1SP PKI RAPP as set out in Annex E of this Policy; and

(ii) in response to a Certificate Signing Request made by an Eligible Subscriber in accordance with the SS1SP PKI RAPP as set out in Annex E of this Policy.

(B) The SS1SPCA shall ensure that:

(i) each SS1SPCA Certificate Issued by it contains information that it has verified to be correct and complete; and

(ii) each SS1SP End Entity Certificate Issued by it contains information consistent with the information in the Certificate Signing Request.

(C) A S1SPCA Certificate may only be:

(i) Issued by the SS1SPCA; and

(ii) for that purpose, signed using the SS1SPCA Root Private Key for the SS1SPCA Intermediate SS1SPCA or the Intermediate SS1SPCA Private Key for the Subordinate SS1SPCA.

(D) A SS1SP End Entity Certificate may only be:

(i) Issued by the Subordinate SS1SPCA; and

(ii) for that purpose, signed using a Subordinate SS1SPCA Private Key.

4.3.2 Notification to Eligible Subscriber by the SS1SPCA of Issuance of Certificate

(A) Provision is made in the SS1SP PKI RAPP as set out in Annex E of this Policy for the SS1SPCA to notify an Eligible Subscriber where that Eligible Subscriber is Issued with a Certificate which was the subject of a Certificate Signing Request made by it.

4.4 Certificate Acceptance

4.4.1 Conduct Constituting Certificate Acceptance

(A) A Certificate which has been Issued by the SS1SPCA shall be treated as valid for any purposes of this Policy until it is treated as having been rejected by the Eligible Subscriber to which it was Issued.

(B) The SS1SPCA shall maintain a record of all Certificates which have been Issued by it and are treated as accepted by a Subscriber.

(C) Further provision in relation to the rejection and acceptance of Certificates is set out in Annex C of this Policy.

4.4.2 Publication of Certificates by the SS1SPCA

(A) Provision in relation to the publication of Certificates is made in Part 2 of this Policy.

4.4.3 Notification of Certificate Issuance by the SS1SPCA to Other Entities

(A) The SS1SPCA shall not give notice of the Issue of a Certificate to any Other Entities.

4.5 KEY PAIR AND CERTIFICATE USAGE

4.5.1 Subscriber Private Key and Certificate Usage

(A) Provision for restrictions on the use by Subscribers of Private Keys in respect of Certificates is made in Annex C: Subscriber Obligations of this Policy.

4.5.2 Relying Party Public Key and Certificate Usage

(A) Provision in relation to reliance that may be placed on a Certificate is made in the Relying Party Obligations as set out in Annex D of this Policy.

4.6 Certificate renewal

(A) This Policy does not support Certificate Renewal.

(B) The SS1SPCA shall not provide a Certificate Renewal service.

(C) Where a new Key Pair has been generated the Eligible Subscriber shall apply for the Issue of a new Certificate in accordance with this Part 4.7 of this Policy.

4.6.1 Who may Request Certification of a New Public Key

[*Not applicable in this Policy*]

4.6.2 Processing Certificate Renewal Requests

[*Not applicable in this Policy*]

4.6.3 Notification of New Certificate Issuance to Subscriber

[*Not applicable in this Policy*]

4.6.4 Conduct Constituting Acceptance of a Renewal Certificate

[*Not applicable in this Policy*]

4.6.5 Publication of the Renewal Certificate by the SS1SPCA

[*Not applicable in this Policy*]

4.6.6 Notification of Certificate Issuance by the SS1SPCA to Other Entities

[*Not applicable in this Policy*]

4.7 Certificate Re-key

4.7.1 Circumstances of Certificate re-key

(A) This Policy provides support for Certificate re-key.

(B) The SS1SPCA may only re-key Certificates in accordance with Part 3.3.1 (B) of this Policy.

(C) The SS1SPCA shall not provide support for re-key of Certificates other than those outlined in Part 3.3.1 (B), or where any Certificate is compromised (or is suspected of being) in accordance with Secure S1SP's BC/DR plans as per Part 5.7 of this Policy.

4.7.2 Circumstances of Certificate Re-key

(A) An Eligible Subscriber may apply for a Certificate to be re-keyed where either:

(i) the SS1SP End Entity Private Key associated with the Certificate has expired; or

(ii) the SS1SPCA Private Key associated with the SS1SPCA Certificate has been Compromised (or is suspecting of being) in accordance with Part 5.7 of this Policy.

(B) In relation to Part 4.7.2 (A)(i) above, the SS1SP End Entity Certificates that can be re-keyed under normal operating conditions are set out in Part 3.3.1 (B) of this policy.

4.7.3 Who May Request a Re-keyed Certificate

(A) In accordance with Part 4.7.2 (B), an Eligible Subscriber may request a Certificate re-key at any time by applying for the Issue of a new SS1SP End Entity Certificate in accordance with this Policy.

4.7.4 Processing Re-keyed Certificate Requests

(A) See Part 4.2 of this Policy

4.7.5 Notification of Re-keyed Certificate Issuance to a Subscriber

(A) See Part 4.3.2 of this Policy.

4.7.6 Conduct Constituting Acceptance of a Re-keyed Certificate

(A) See Part 4.4.1 of this Policy.

4.7.7 Publication of a Re-keyed Certificate by the SS1SPCA

(A) See Part 4.4.2 of this Policy.

4.7.8 Notification of Re-keyed Certificate Issuance by the SS1SPCA to Other Entities

(A) See Part 4.4.3 of this Policy

4.8 Certificate modification

4.8.1 Circumstances for Certificate Modification

(A) This Policy does not support Certificate modification.

(B) Neither the SS1SPCA nor any Subscriber may modify a Certificate.

4.8.2 Who may request Certificate Modification

[*Not applicable in this Policy*]

4.8.3 Processing Certificate Modification Requests

[*Not applicable in this Policy*]

4.8.4 Notification of New Certificate Issuance to Subscriber

[*Not applicable in this Policy*]

4.8.5 Conduct Constituting Acceptance of Modified Certificate

[*Not applicable in this Policy*]

4.8.6 Publication of the Modified Certificate by the SS1SPCA

[*Not applicable in this Policy*]

4.8.7 Notification of Certificate Issuance by the SS1SPCA to Other Entities

[*Not applicable in this Policy*]

4.9 Certificate revocation and suspension

4.9.1 Circumstances for Revocation

(A) This Policy does not support the revocation or suspension of Certificates.

(B) The SS1SPCA shall not provide any service of revoking or suspending a Certificate.

4.9.2 Who can Request Revocation

[*Not applicable in this Policy*]

4.9.3 Procedure for Revocation Request

[*Not applicable in this Policy*]

4.9.4 Revocation Request Grace Period

[*Not applicable in this Policy*]

4.9.5 Time within which SS1SPCA must process the Revocation Request

[*Not applicable in this Policy*]

4.9.6 Revocation Checking Requirements for Relying Parties

[*Not applicable in this Policy*]

4.9.7 CRL Issuance Frequency (if applicable)

[*Not applicable in this Policy*]

4.9.8 Maximum Latency for CRLs (if applicable)

[*Not applicable in this Policy*]

4.9.9 On-line Revocation/Status Checking Availability

[*Not applicable in this Policy*]

4.9.10 On-line Revocation Checking Requirements

[*Not applicable in this Policy*]

4.9.11 Other Forms of Revocation Advertisements Available

[*Not applicable in this Policy*]

4.9.12 Special Requirements in the Event of Key Compromise

See Part 4.7.2 of this Policy.

4.9.13 Circumstances for Suspension

[*Not applicable in this Policy*]

4.9.14 Who can Request Suspension

[*Not applicable in this Policy*]

4.9.15 Procedure for Suspension Request

[*Not applicable in this Policy*]

4.9.16 Limits on Suspension Period

[*Not applicable in this Policy*]

4.10 Certificate status services

4.10.1 Operational Characteristics

[*Not applicable in this Policy*]

4.10.2 Service Availability

[*Not applicable in this Policy*]

4.10.3 Optional Features

[*Not applicable in this Policy*]

4.11 End of subscription

[*Not applicable in this Policy*]

4.12 Key Escrow and recovery

4.12.1 Key Escrow and Recovery Policies and Practices

(A) The SS1SPCA PKI does not provide Key Escrow services.

(B) SS1SPCA recovery policies and practices are documented in the SS1SP CPS.

4.12.2 Session Key Encapsulation and Recovery Policy and Practices

(A) The SS1SPCA PKI does not provide Session Key encapsulation services.

(B) SS1SPCA recovery policies and practices are documented in the SS1SP CPS.

5 Facility management and operational controls

5.1 PHYSICAL CONTROLS

5.1.1 Site Location and Construction

(A) The Secure S1SP shall ensure that the SS1SPCA Systems are operated in a sufficiently secure environment, where the Secure S1SP will comply with or achieve certification with the following standard of the International Organisation for Standards in respect of the security, reliability and resilience of its information assets and processes, where the scope will be sufficient enough to include the SS1SPCA PKI:

(i) ISO/IEC 27001:2013 (Information Technology - Security Techniques - Information Security Management Systems); or
(ii) any equivalent to that standard which updates or replaces it from time to time.

(B) The SS1SPCA shall ensure that:

(i) all of the physical locations in which the SS1SPCA Systems are situated, operated, routed or directly accessed are in the United Kingdom or India;

(ii) all bespoke Security Related Functionality is developed, specified, designed, built and tested only within the United Kingdom or India; and

(iii) all Security Related Functionality is integrated, configured, tested in situ, implemented, operated and maintained only within the United Kingdom or India.

(C) The SS1SPCA shall ensure that the SS1SPCA Systems cannot be indirectly accessed from any location outside the United Kingdom or India.

(D) The SS1SPCA shall ensure that the SS1SP CPS incorporates provisions designed to ensure that all physical locations in which the manufacture of Certificates and Time-Stamping take place are at all times manually or electronically monitored for unauthorised intrusion in accordance with ISO/IEC 27001:2013 (Information Technology – Security Techniques – Information Security Management Systems) and industry good practice.

(E) The SS1SPCA shall ensure that, where applicable, the SS1SP CPS incorporates provisions designed to ensure that all PINs, pass-phrases and passwords used for the purposes of carrying out the cryptographic and sensitive functions of the SS1SPCA are stored securely, are encrypted and are accessible only to SS1SPCA Personnel in Privileged Roles.

5.1.2 Physical Access

(A) The SS1SPCA shall ensure that the SS1SP CPS incorporates provisions in relation to access control, including in particular provisions designed to:

(i) establish controls such that only appropriately authorised personnel may have unescorted physical access to SS1SPCA Systems, or any System used for the purposes of Time-Stamping;

(ii) ensure that any unauthorised personnel may have physical access to such Systems only if appropriately authorised and supervised;

(iii) ensure that a site access log is both maintained and periodically inspected for all locations at which such Systems are sited; and

(iv) ensure that all removable media which contain sensitive plain text Data and are kept at such locations are stored in secure containers accessible only to appropriately authorised individuals.

5.1.3 Power and Air Conditioning

(A) The SS1SPCA shall ensure that the SS1SP CPS incorporates provisions in relation to power and air conditioning at all physical locations in which the SS1SPCA Systems are situated.

5.1.4 Water Exposure

(A) The SS1SPCA shall ensure that the SS1SP CPS incorporates provisions in relation to water exposure at all physical locations in which the SS1SPCA Systems are situated.

5.1.5 Fire Prevention and Protection

(A) The SS1SPCA shall ensure that the SS1SP CPS incorporates provisions in relation to fire prevention and protection at all physical locations in which the SS1SPCA Systems are situated.

5.1.6 Media Storage

(A) The SS1SPCA shall ensure that the SS1SP CPS incorporates provisions designed to ensure that appropriate controls are placed on all media used for the storage of Data held by it for the purposes of carrying out its functions as the SS1SPCA.

5.1.7 Waste Disposal

(A) The SS1SPCA shall ensure that all media used to store Data held by it for the purposes of carrying out its functions as the SS1SPCA are disposed of only using secure methods of disposal in accordance with good industry practice.

5.1.8 Off-Site Back-Up

(A) The SS1SPCA shall regularly carry out a Back-Up of:

(i) all Data held on the SS1SPCA Systems which are critical to the operation of those Systems or continuity in the provision of the SS1SP PKI Services; and

(ii) all other sensitive Data.

(B) For the purposes of paragraph (A), the SS1SPCA shall ensure that the SS1SP CPS incorporates provisions which identify the categories of critical and sensitive Data that are to be Backed-Up.

(C) The SS1SPCA shall ensure that Data which are Backed-Up in accordance with paragraph (A):

(i) are stored on media that are located in physically secure facilities in different locations to the sites at which the Data being Backed-Up are ordinarily held;

(ii) are protected in accordance with the outcome of a risk assessment, including when being transmitted for the purposes of Back-Up; and

(iii) to the extent to which they comprise SS1SPCA Private Key Material, are Backed-Up:

(a) to appropriate Security Containers which are stored off-line in encrypted format.

(D) The SS1SPCA shall ensure that, where any elements of the SS1SPCA Systems, any Data held for the purposes of providing the SS1SP PKI Services, or any items of SS1SPCA equipment are removed from their primary location, they continue to be protected in accordance with the security standard appropriate to the primary location.

(E) The SS1SPCA will ensure that the SS1SP CPS incorporates provisions in relation to paragraphs (A), (B), (C) and (D) above.

5.2 Procedural controls

5.2.1 Trusted Roles

(A) The SS1SPCA shall ensure that:

(i) no individual may carry out any activity which involves access to resources, or Data held on the SS1SPCA Systems unless that individual has been expressly authorised to have such access;

(ii) each member of SS1SPCA Personnel has a clearly defined level of access to the SS1SPCA Systems and the premises in which they are located;

(iii) no individual member of SS1SPCA Personnel is capable, by acting alone, of engaging in any action by means of which the SS1SPCA Systems may be Compromised to a material extent; and

(iv) the SS1SP CPS incorporates provisions designed to ensure that appropriate controls are in place for the purposes of compliance by the SS1SPCA with the requirements of this Part 5.2.1 of this Policy.

5.2.2 Number of Persons Required per Task

(A) The SS1SPCA shall ensure that the SS1SP CPS incorporates provisions designed to establish:

(i) the appropriate separation of roles between the different members of SS1SPCA Personnel; and

(ii) the application of controls to the actions of all members of SS1SPCA Personnel who are Privileged Users, identifying in particular any controls designed to ensure that the involvement of more than one individual is required for the performance of certain functions where reasonably practicable.

(B) The SS1SPCA shall ensure that the SS1SP CPS, as a minimum, makes provision for the purposes of paragraph (A) in relation to the following areas:

(i) SS1SPCA Systems administration;

(ii) SS1SPCA Systems operations;
(iii) SS1SPCA Systems security; and
(iv) SS1SPCA Systems auditing.

5.2.3 Identification and Authentication for Each Role

(A) See Part 5.2.2 of this Policy.

5.2.4 Roles Requiring Separation of Duties

(A) See Part 5.2.2 of this Policy.

5.3 Personnel controls

5.3.1 Qualification, Experience and Clearance Requirements

(A) The SS1SPCA shall ensure that all SS1SPCA Personnel must:

(i) be appointed to their roles in writing;

(ii) be bound by contract to the terms and conditions relevant to their roles;

(iii) have received appropriate training with respect to their duties;

(iv) be bound by contract not to disclose any confidential, sensitive, personal or security-related Data except to the extent necessary for the performance of their duties or for the purposes of complying with any requirement of law; and

(v) in so far as can reasonably be ascertained by the SS1SPCA, not have been previously relieved of any past assignment (whether for the SS1SPCA or any other person) on the grounds of negligence or any other failure to perform a duty.

(B) The SS1SPCA shall ensure that all SS1SPCA Personnel have, as a minimum, passed an industry recognised and assured security check before commencing their roles.

5.3.2 Background Check Procedures

(A) See Part 5.3.1 of this Policy.

5.3.3 Training Requirements

(A) See Part 5.3.1 of this Policy.

5.3.4 Retraining Frequency and Requirements

(A) The SS1SPCA shall ensure that the SS1SP CPS incorporates appropriate provisions relating to the frequency and content of retraining and refresher training to be undertaken by members of SS1SPCA Personnel.

5.3.5 Job Rotation Frequency and Sequence

(A) The SS1SPCA shall ensure that the SS1SP CPS incorporates appropriate provisions relating to the frequency and sequence of job rotations to be undertaken by members of SS1SPCA Personnel.

5.3.6 Sanctions for Unauthorised Actions

(A) The SS1SPCA shall ensure that the SS1SP CPS incorporates appropriate provisions relating to sanctions for unauthorised actions undertaken by members of SS1SPCA Personnel.

5.3.7 Independent Contractor Requirements

(A) References to the SS1SPCA in this Policy include references to persons with whom the SS1SPCA contracts in order to secure performance of its obligations as the SS1SPCA.

5.3.8 Documentation Supplied to Personnel

(A) The SS1SPCA shall ensure that all SS1SPCA Personnel are provided with access to all documents relevant to their roles or necessary for the performance of their duties, including in particular:

(i) this Policy;

(ii) the SS1SP CPS; and

(iii) any supporting documentation, statutes, policies or contracts.

5.4 Audit logging procedures

5.4.1 Types of Events Recorded

(A) The SS1SPCA shall ensure that:

(i) the SS1SPCA Systems record all systems activity in an audit log;

(ii) the SS1SP CPS incorporates a comprehensive list of all events that are to be recorded in an audit log in relation to:

(a) the activities of SS1SPCA Personnel;

(b) the use of SS1SPCA equipment;

(c) the use of (including both authorised and unauthorised access, and attempted access to) any premises at which functions of the SS1SPCA are carried out;

(d) communications and activities that are related to the Issue of Certificates (in so far as not captured by the SS1SPCA Systems audit log); and

(e) it records in an audit log all the events specified in paragraph (ii).

5.4.2 Frequency of Processing Log

(A) The SS1SPCA shall ensure that:

(i) the audit logging functionality in the SS1SPCA Systems is fully enabled at all times;

(ii) all SS1SPCA Systems activity recorded in the Audit Log is recorded in a standard format that is aligned with:

(a) British Standard BS 10008:2008 (Evidential Weight and Legal Admissibility of Electronic Information); or

(b) any equivalent to that British Standard which updates or replaces it from time to time.

(B) The SS1SPCA shall ensure that the SS1SP CPS incorporates provisions which specify:

(i) how regularly information recorded in the Audit Log is to be reviewed; and

(ii) what actions are to be taken by it in response to types of events recorded in the Audit Log.

(C) The SS1SPCA shall ensure that the SS1SP CPS incorporates provisions in relation to access to the Audit Log, providing in particular that:

(i) Data contained in the Audit Log must not be accessible other than on a read-only basis; and

(ii) access to those Data must be limited to those members of SS1SPCA Personnel who are performing a dedicated system audit role.

5.4.3 Retention Period for Audit Log

(A) The SS1SPCA shall:

(i) retain the Audit Log so that it incorporates, on any given date, a record of all system events occurring during a period of at least twelve months prior to that date; and

(ii) ensure that a copy of the Audit Log incorporating a record of all system events occurring prior to the beginning of that period is archived in accordance with the requirements of Part 5.5 of this Policy.

5.4.4 Protection of Audit Log

(A) The SS1SPCA shall ensure that:

(i) to the extent to which the Audit Log is retained electronically, the Data stored in it cannot be accessed other than on a read-only basis, and are protected from unauthorised viewing, modification and deletion in accordance with:

(a) British Standard BS 10008:2008 (Evidential Weight and Legal Admissibility of Electronic Information); or

(b) any equivalent to that British Standard which updates or replaces it from time to time; and

(c) to the extent to which the Audit Log is retained in non-electronic form, the Data stored in it are appropriately protected from unauthorised viewing, modification and destruction in order to ensure that their integrity is maintained for evidential purposes.

5.4.5 Audit Log Back-Up Procedures

(A) The SS1SPCA shall ensure that the Data contained in the Audit Log are Backed-Up (or, to the extent that the Audit Log is retained in non-electronic form, are copied):

(i) on a daily basis; or

(ii) if activity has taken place on the SS1SPCA Systems only infrequently, in accordance with the schedule for the regular Back-Up of the Data held on those Systems.

(B) The SS1SPCA shall ensure that all Data contained in the Audit Log which are Backed-Up are, during Back-Up:

(i) held in accordance with the outcome of a risk assessment which is documented in the SS1SP CPS; and

(ii) protected to the same standard of protection as the primary copy of the Audit Log in accordance with Part 5.4.4 of this Policy.

5.4.6 Audit Collection System (Internal or External)

(A) The SS1SPCA shall ensure that the SS1SP CPS incorporates provisions in relation to its system for collecting Data for the purpose of populating the Audit Log.

5.4.7 Notification to Event-Causing Subject

(A) The SS1SPCA shall ensure that the SS1SP CPS incorporates provisions in relation to its notification of any person who is (or is responsible for any System which is) the direct cause of an event recorded in the Audit Log.

5.4.8 Vulnerability Assessments

(A) Provision is made in the SS1SP CPS in relation to the carrying out of vulnerability assessments in respect of the SS1SPCA Systems.

5.5 Records Archival

5.5.1 Types of Records Archived

(A) The SS1SPCA shall ensure that it archives:

(i) the Audit Log in accordance with Part 5.4.3 of this Policy;

(ii) its records of all Data submitted to it by Eligible Subscribers for the purposes of Certificate Signing Requests; and

(iii) any other Data specified in this Policy as requiring to be archived in accordance with this Part 5.5.

5.5.2 Retention Period for Archive

(A) Where there is a need to Archive Data, the SS1SPCA shall ensure that any Data which is to be Archived is retained in accordance with their Data Retention and Destruction Policy.

5.5.3 Protection of Archive

(A) The SS1SPCA shall ensure that the SS1SP CPS details how Data held in its Archive are:

(i) protected against any unauthorised access;

(ii) adequately protected against environmental threats such as temperature, humidity and magnetism; and

(iii) incapable of being modified or deleted.

5.5.4 Archive Back-Up Procedures

(A) The SS1SPCA shall ensure that the SS1SP CPS incorporates provisions in relation to its procedures for the Back-Up of its Archive.

5.5.5 Requirements for Time-Stamping of Records

(A) Provision in relation to Time-Stamping is made in Part 6.8 of this Policy.

5.5.6 Archive Collection System (Internal or External)

(A) The SS1SPCA shall ensure that the SS1SP CPS incorporates provisions in relation to its system for collecting Data for the purpose of populating the Archive.

5.5.7 Procedures to Obtain and Verify Archive Information

(A) The SS1SPCA shall ensure that:

(i) Data held in the Archive are stored in a readable format during their retention period; and

(ii) those Data remains accessible at all times during their retention period, including during any period of interruption, suspension or cessation of the SS1SPCA's operations.

(B) The SS1SPCA shall ensure that the SS1SP CPS incorporates provisions in relation to the periodic verification by the SS1SPCA of the Data held in the Archive.

5.6 Key changeover

5.6.1 SS1SP End Entity Certificate Key Changeover

(A) The SS1SPCA shall only ever Issue a new SS1SP End Entity Certificate for those SS1SP End Entity Certificates as described in Part 3.3.1 (B) of this Policy, and where a new Certificate Signing Request is submitted by an Eligible Subscriber in accordance with the requirements of the SS1SP PKI RAPP as set out in Annex E of this Policy and Part 4.7 of this Policy.

5.7 Compromise and disaster recovery

5.7.1 Incident and Compromise Handling Procedures

(A) The SS1SPCA shall ensure that the SS1SP CPS incorporates a business continuity plan which shall be designed to ensure continuity in, or (where there has been unavoidable discontinuity) the recovery of, the provision of the SS1SP PKI Services in the event of any security compromise of the SS1SPCA Systems or major failure in the SS1SPCA processes.

(B) The SS1SPCA shall ensure that the procedures set out in the business continuity plan are:

(i) aligned with ISO 22301 and ISO 27031 (or any equivalent to those standards which update or replace them from time to time); and

(ii) tested periodically, and in any event at least once in each year, in order to ensure that they are operationally effective.

(C) The SS1SPCA shall ensure that the SS1SP CPS incorporates provisions setting out the approach to be taken by it in circumstances in which it suspects (or has reason to suspect) that any SS1SPCA Private Key or any part of the SS1SPCA Systems is Compromised.

5.7.2 Computing Resources, Software and/or Data are Corrupted

(A) The SS1SPCA shall ensure that the business continuity plan established in accordance with Part 5.7.1 of this Policy incorporates provisions setting out the steps to be taken in the event of any loss of or corruption to computing resources, software or Data.

5.7.3 Entity Private Key Compromise Procedures

(A) See Part 5.7.1 of this Policy.

5.7.4 Business Continuity Capabilities after a Disaster

(A) The SS1SPCA shall ensure that the business continuity plan established in accordance with Part 5.7.1 of this Policy is designed to ensure the recovery of the provision of the SS1SP PKI Services within not more than 48 hours of the occurrence of any event causing discontinuity.

5.8 Certification authority and registration authority termination

[*Not applicable in this Policy*]

6 Technical security controls

(A) The SS1SPCA shall ensure that the SS1SP CPS incorporates detailed provision in relation to the technical controls to be established and operated for the purposes of the exercise of its functions as the SS1SPCA.

6.1 Key pair generation and installation

6.1.1 Key Pair Generation

(A) The SS1SPCA shall ensure that all SS1SPCA Key which it uses for the purposes of this Policy are generated in accordance with Part 6.1.1 of the SS1SP CPS.

(B) The SS1SPCA shall not generate any Private Key or Public Key other than a SS1SPCA Key.

(C) The SS1SPCA shall ensure that all SS1SPCA Private Keys that are not required for continuous operational purposes will be encrypted and stored securely in an off-line security container which requires M of N to activate the SS1SPCA Private Key when required.

6.1.2 Private Key Delivery to Subscriber

(A) In accordance with Part 6.1.1(B), the SS1SPCA shall not generate any Private Key for delivery to a Subscriber.

6.1.3 Public Key Delivery to Certificate Issuer

(A) The SS1SPCA shall ensure that the SS1SP CPS incorporates provisions:

(i) in relation to the mechanism by which Public Keys of Subscribers are delivered to it for the purpose of the exercise of its functions as the Root SS1SPCA, Intermediate SS1SPCA and Subordinate SS1SPCA; and

(ii) ensuring that the mechanism uses a recognised standard protocol such as PKCS#10.

6.1.4 SS1SPCA Public Key Delivery to Relying Parties

(A) The SS1SPCA shall ensure that the SS1SP CPS incorporates provisions:

(i) in relation to the manner by which each SS1SPCA Public Key is to be lodged in the SS1SP PKI Repository; and

(ii) designed to ensure that the SS1SPCA Public Keys are securely lodged in the SS1SP PKI Repository in such a manner as to guarantee that their integrity is maintained.

6.1.5 Key Sizes

(A) The SS1SPCA and every Subscriber shall ensure that all Private Keys and Public Keys which each of them may use for the purposes of this Policy are of the size and characteristics set out in Annex B to this Policy.

6.1.6 Public Key Parameters Generation and Quality Checking

(A) The SS1SPCA shall ensure that any Public Key used by it for the purposes of this Policy shall be of values and lengths that make the success of known attacks infeasible.

(B) Each Subscriber shall ensure that any Public Key used by it for the purposes of this Policy shall be of values and lengths that make the success of known attacks infeasible.

6.1.7 Key Usage Purposes (as per X.509 v3 keyUsage Field)

(A) The SS1SPCA shall ensure that each Certificate that is Issued by it has a `keyUsage` field in accordance with RFC5759 and RFC5280.

(B) The SS1SPCA shall ensure that each SS1SPCA Certificate andSS1SP End Entity Certificate that is Issued by it, is in accordance with the SS1SPCA Certificate Profiles and the SS1SP End Entity Certificate Profiles in Annex B.

6.2 Private Key Protection and Cryptographic Module Engineering Controls

6.2.1 Cryptographic Module Standards and Controls

(A) The SS1SPCA shall ensure that all SS1SPCA Private Keys shall be:

(i) protected to a high standard of assurance by physical and logical security controls;

(ii) stored in Security Containers and operated in accordance with Part 6.2.1 of the SS1SP CPS; and

(iii) enforce M of N controls to activate the SS1SPCA Private Key.

(B) The SS1SPCA shall ensure that all SS1SPCA Private Keys shall, where they affect the outcome of any Certificates Issued by it, be protected by, stored in and operated in accordance with Part 6.2.1 of the SS1SP CPS.

(C) The SS1SPCA shall ensure that no SS1SPCA Private Key shall be made available in either complete or unencrypted form in accordance with Part 6.2.1 of the SS1SP CPS.

(D) The SS1SPCA shall ensure that any secure mechanism which is used for any purpose related to Certificate life-cycle management shall:

(a) operate so as to block access to itself following a number of failed consecutive attempts to access it using Activation Data, where that number shall be set out in the SS1SP CPS; and

(b) require to be unblocked by an authorised member of SS1SPCA Personnel who has been Authenticated as such following a process which shall be set out in the SS1SP CPS.

6.2.2 Private Key (m out of n) Multi-Person Control

(A) The SS1SPCA shall ensure that the SS1SP CPS incorporates provisions for the exercise of strict controls in relation to Private Key (m out of n) Multi-Person Control.

6.2.3 Private Key Escrow

(A) This Policy does not support Key Escrow.

(B) The SS1SPCA shall not provide any Key Escrow service.

6.2.4 Private Key Back-Up

(A) The SS1SPCA may Back-Up SS1SPCA Private Keys insofar as:

(i) each Private Key is protected to a standard which is at least equivalent to that required in relation to the principal Private Key in accordance with this Policy; and

(ii) where more than one Private Key is Backed-Up within a single security environment, each of the Private Keys which is Backed-Up within that environment must be protected to a standard which is at least equivalent to that required in relation to an SS1SPCA Private Key in accordance with this Policy.

6.2.5 Private Key Archival

(A) The SS1SPCA shall ensure that no SS1SPCA Key, which is a Private Key, is archived.

6.2.6 Private Key Transfer into or from a Cryptographic Module

(A) The SS1SPCA shall ensure that no SS1SPCA Private Key is transferred or copied other than:

(i) for the purposes of:

(a) Back-Up; or

(b) establishing an appropriate degree of resilience in relation to the provision of the SS1SP PKI Services; and

(ii) kept secure and encrypted within a Security Container, with appropriate access controls enforced at all times.

6.2.7 Private Key Storage on Cryptographic Module

(A) See Part 6.2.1 of this Policy.

6.2.8 Method of Activating Private Key

(A) The SS1SPCA shall ensure that the Security Container in which any SS1SPCA Private Key is stored may be accessed only by an authorised member of SS1SPCA Personnel who has been Authenticated following an Authentication process which:

(i) has an appropriate level of strength to ensure the commensurate protection of the Private Key;

(ii) involves the use of Activation Data; and

(iii) requires M of N access to activate the SS1SPCA Private Key within the Security Container.

6.2.9 Method of Deactivating Private Key

(A) The SS1SPCA shall ensure that any SS1SPCA Private Key shall be capable of being de-activated by means of the SS1SPCA Systems, at least by:

(i) the actions of:

(a) turning off the power;

(b) logging off;

(c) carrying out a system reset; and

(ii) a period of inactivity of a length which shall be set out in the SS1SP CPS.

6.2.10 Method of Destroying Private Key

(A) The SS1SPCA shall ensure that the SS1SP CPS incorporates provisions for the exercise of strict controls in relation to the destruction of SS1SPCA Keys.

(B) The SS1SPCA shall ensure that no SS1SPCA Key (whether in active use, existing as a copy for the purposes of resilience, or Backed-Up) is destroyed except in accordance with a positive decision by the SSC for PKI instructing the SS1SPCA to destroy it.

6.2.11 Cryptographic Module Rating

(A) See Part 6.2.1 of this Policy.

6.3 OTHER ASPECTS OF KEY PAIR MANAGEMENT

6.3.1 Public Key Archival

(A) The SS1SPCA shall ensure that, where necessary, it archives SS1SPCA Public Keys in accordance with the requirements of Part 5.5 of this Policy.

6.3.2 Certificate Operational Periods and Key Pair Usage Periods

(A) The SS1SPCA shall ensure that:

(i) the Validity Period of each Certificate, unless explicitly documented otherwise in Annex B, shall be an indefinite period; and

(ii) for this purpose, it uses the notAfter value specified in Annex B.

6.4 Activation data

6.4.1 Activation Data Generation and Installation

(A) The SS1SPCA shall ensure that any secure container within which a SS1SPCA Key is held has Activation Data that are unique and unpredictable.

(B) The SS1SPCA shall ensure that:

(i) these Activation Data, in conjunction with any other access control, shall be of an appropriate level of strength for the purposes of protecting the SS1SPCA Keys; and

(ii) where the Activation Data comprise any PINs, passwords or passphrases, the SS1SPCA shall have the ability to change these at any time.

6.4.2 Activation Data Protection

(A) The SS1SPCA shall ensure that the SS1SP CPS incorporates provision for the use of such cryptographic protections and access controls as are appropriate to protect against the unauthorised use of Activation Data.

6.4.3 Other Aspects of Activation Data

[*Not applicable in this Policy*]

6.5 Computer security controls

6.5.1 Specific Computer Security Technical Requirements

(A) The SS1SPCA shall ensure that the SS1SP CPS incorporates provisions in relation to the identification and implementation, following the conclusion of any threat assessment, of security measures which make provision for at least the following:

(i) the establishment of access controls in relation to the activities of the SS1SPCA;

(ii) the appropriate allocation of responsibilities to Privileged Users;

(iii) the identification and Authentication of organisations, individuals and Systems involved in SS1SPCA activities;

(iv) the use of cryptography for communication and the protection of Data stored on the SS1SPCA Systems;

(v) the audit of security related events; and

(vi) the use of recovery mechanisms for SS1SPCA Keys.

6.6 Life cycle technical controls

6.6.1 System Development Controls

(A) The SS1SPCA shall ensure that any software which is developed for the purpose of establishing a functionality of the SS1SPCA Systems shall:

(i) take place in a controlled environment that is sufficient to protect against the insertion into the software of malicious code;

(ii) be undertaken by a developer which has a quality system that is:

(a) compliant with recognised international standards (such as ISO 9001:2000 or an equivalent standard); or

(b) available for inspection and approval by the SSC for PKI and has been so inspected and approved.

6.6.2 Security Management Controls

(A) The SS1SPCA shall ensure that the SS1SP CPS incorporates provisions which are designed to ensure that the SS1SPCA Systems shall comply with or achieve certification with the following standard of the International Organisation for Standards in respect of the security, reliability and resilience of its information assets and processes and its SS1SPCA Systems:

(i) ISO/IEC 27001:2013 (Information Technology – Security Techniques – Information Security Management Systems); or

(ii) any equivalent to that standard which updates or replaces it from time to time.

6.6.3 Life-Cycle Security Controls

(A) See Part 6.6.2 of this Policy.

6.7 Network security controls

6.7.1 Use of Offline Root SS1SPCA and Intermediate SS1SPCA

(A) The SS1SPCA shall ensure that its functions as the Root SS1SPCA and Intermediate SS1SPCA are carried out on a part of the SS1SPCA Systems that is neither directly nor indirectly connected to any System which is not a part of the SS1SPCA Systems.

(B) The SS1SPCA CPS will provide further detail with respect to SS1SPCA network security controls.

6.7.2 Protection Against Attack

(A) The SS1SPCA shall use its best endeavours to ensure that the SS1SPCA Systems are not Compromised, and in particular for this purpose that they are designed and operated so as to detect and prevent:

(i) any Denial of Service Event;

(ii) any unauthorised attempt to connect to them.

(B) The SS1SPCA shall take reasonable steps to ensure that the SS1SPCA Systems cause or permit to be open at any time only those network ports, and allow only those protocols, which are required at that time for the effective operation of those Systems, and block all network ports and protocols which are not so required.

6.7.3 Separation of Subordinate SS1SPCA

(A) The DCC shall ensure that, where any Subordinate SS1SPCA functions are carried out on a System that is connected to an external network, they are carried out on a System that is Separated from all other SS1SPCA Systems.

6.7.4 Health Check of SS1SPCA Systems

(A) The SS1SPCA shall ensure that, in relation to the SS1SPCA Systems, a vulnerability assessment in accordance with the SS1SP CPS and is carried out with such frequency as may be specified from time to time by the Independent S1SPKM Assurance Service Provider.

6.8 Time-stamping

6.8.1 Use of Time-Stamping

(A) The SS1SPCA shall ensure that Time-Stamping takes place in relation to all Certificates and all other SS1SPCA activities which require an accurate record of time.

(B) The SS1SPCA shall ensure that the SS1SPCA incorporates provisions in relation to the time source and mechanisms used by any Time-Stamping Authority which carries out Time-Stamping on behalf of the SS1SPCA.

7 CERTIFICATE, CRL AND OCSP PROFILES

7.1 CERTIFICATE PROFILES

The SS1SPCA shall use only the Certificate Profiles in Annex B.

7.1.1 Version Number(s)

[*Not applicable in this Policy*]

7.1.2 Certificate Extensions

[Not applicable in this Policy]

7.1.3 Algorithm Object Identifiers

[Not applicable in this Policy]

7.1.4 Name Forms

[Not applicable in this Policy]

7.1.5 Name Constraints

[Not applicable in this Policy]

7.1.6 Certificate Policy Object Identifier

[Not applicable in this Policy]

7.1.7 Usage of Policy Constraints Extension

[Not applicable in this Policy]

7.1.8 Policy Qualifiers Syntax and Semantics

[Not applicable in this Policy]

7.1.9 Processing Semantics for the Critical Certificate Policies Extension

[Not applicable in this Policy]

7.2 CRL PROFILE

7.2.1 Version Number(s)

[Not applicable in this Policy]

7.2.2 CRL and CRL Entry Extensions

[Not applicable in this Policy]

7.3 OCSP PROFILE

7.3.1 Version Number(s)

[Not applicable in this Policy]

7.3.2 OCSP Extensions

[Not applicable in this Policy]

8 Compliance audit and other assessments

8.1 Frequency or circumstances of assessment

(A) Provision in relation to this is made in the SS1SP CPS.

8.2 Identity/qualifications of assessor

(A) Provision in relation to this is made in the SS1SP CPS.

8.3 Assessor’s relationship to assessed entity

(A) Provision in relation to this is made in the SS1SP CPS.

8.4 Topics covered by assessment

(A) Provision in relation to this is made in the SS1SP CPS.

8.5 Actions taken as a result of deficiency

(A) Provision in relation to this is made in the SS1SP CPS.

8.6 Communication results

(A) Provision in relation to this is made in the SS1SP CPS.

9 Other business and legal matters

(A) In so far as provision is made in relation to any or all the matters referred to in this Part, these can be found in the S1SP commercial contracts, this Policy and the provisions of Annex C: Subscriber Obligations of this Policy and Annex D: Relying Party Obligations of this Policy.

9.1 Fees

[Not applicable in this Policy]

9.1.1 Certificate Issuance or Renewal Fees

[Not applicable in this Policy]

9.1.2 SS1SP End Entity Certificate Access Fees

[Not applicable in this Policy]

9.1.3 Revocation or Status Information Access Fees

[Not applicable in this Policy]

9.1.4 Fees for Other Services

[Not applicable in this Policy]

9.1.5 Refund Policy

[Not applicable in this Policy]

9.2 FINANCIAL RESPONSIBILITY

9.2.1 Insurance Coverage

[Not applicable in this Policy]

9.2.2 Other Assets

[Not applicable in this Policy]

9.2.3 Insurance or Warranty Coverage for Subscribers and Subjects

[Not applicable in this Policy]

9.3 CONFIDENTIALITY OF BUSINESS INFORMATION

9.3.1 Scope of Confidential Information

[Not applicable in this Policy]

9.3.2 Information not within the Scope of Confidential Information

[Not applicable in this Policy]

9.3.3 Responsibility to Protect Confidential Information

[Not applicable in this Policy]

9.4 PRIVACY OF PERSONAL INFORMATION

9.4.1 Privacy Plan

[Not applicable in this Policy]

9.4.2 Information Treated as Private

[Not applicable in this Policy]

9.4.3 Information not Deemed Private

[Not applicable in this Policy]

9.4.4 Responsibility to Protect Private Information

[Not applicable in this Policy]

9.4.5 Notice and Consent to Use Private Information

[Not applicable in this Policy]

9.4.6 Disclosure Pursuant to Judicial or Administrative Process

[Not applicable in this Policy]

9.4.7 Other Information Disclosure Circumstances

[Not applicable in this Policy]

9.5 INTELLECTUAL PROPERTY RIGHTS

[Not applicable in this Policy]

9.6 REPRESENTATIONS AND WARRANTIES

9.6.1 Certification Authority Representations and Warranties

[Not applicable in this Policy]

9.6.2 Registration Authority Representations and Warranties

[Not applicable in this Policy]

9.6.3 Subscriber Representations and Warranties

[Not applicable in this Policy]

9.6.4 Relying Party Representations and Warranties

[Not applicable in this Policy]

9.6.5 Representations and Warranties of Other Participants

[Not applicable in this Policy]

9.7 DISCLAIMERS OF WARRANTIES

[Not applicable in this Policy]

9.8 LIMITATIONS OF LIABILITY

[Not applicable in this Policy]

9.9 INDEMNITIES

[Not applicable in this Policy]

9.10 TERM AND TERMINATION

9.10.1 Term

[Not applicable in this Policy]

9.10.2 Termination of SS1SP End Entity Certificate Policy

[Not applicable in this Policy]

9.10.3 Effect of Termination and Survival

[Not applicable in this Policy]

9.11 INDIVIDUAL NOTICES AND COMMUNICATIONS WITH PARTICIPANTS

9.11.1 Subscribers

[Not applicable in this Policy]

9.11.2 SS1SPCA Certification Authority

[Not applicable in this Policy]

9.11.3 9.11.3 Notification

[Not applicable in this Policy]

9.12 AMENDMENTS

9.12.1 Procedure for Amendment

[Not applicable in this Policy]

9.12.2 Notification Mechanism and Period

[Not applicable in this Policy]

9.12.3 Circumstances under which OID Must be Changed

[Not applicable in this Policy]

9.13 DISPUTE RESOLUTION PROVISIONS

[Not applicable in this Policy]

9.14 GOVERNING LAW

[Not applicable in this Policy]

9.15 COMPLIANCE WITH APPLICABLE LAW

[Not applicable in this Policy]

9.16 MISCELLANEOUS PROVISIONS

9.16.1 Entire Agreement

[Not applicable in this Policy]

9.16.2 Assignment

[Not applicable in this Policy]

9.16.3 Severability

[Not applicable in this Policy]

9.16.4 Enforcement (Attorney's Fees and Waiver of Rights)

[Not applicable in this Policy]

9.16.5 Force Majeure

[Not applicable in this Policy]

9.17 OTHER PROVISIONS

9.17.1 SS1SP End Entity Certificate Policy Content

[Not applicable in this Policy]

9.17.2 Third Party Rights

[Not applicable in this Policy]

10 Annex A: Definitions and interpretation

In this Policy, except where the context otherwise requires -

- the expressions in the left-hand column below shall have the meanings given to them in the right hand column below,
- the rule of interpretation set out at Part 1.1 of this Policy shall apply.

Definition	Interpretation
Activation	means the process of making a SS1SPCA Private Key stored available for use.
Activation Data	means any private Data (such as a password or the Data on a smartcard) which are used to access a Security Container.
Archive	means the archive of Data created in accordance with Part 5.5.1 of this Policy (and "**Archives**" and "**Archived**" shall be interpreted accordingly).
Audit Log	means the audit log created in accordance with Part 5.4.1 of this Policy and the SS1SP CPS.
Authentication	means the process of establishing that an individual, organisation, System or Secure SMETS1 Device is what he or it claims to be (and "**Authenticate**" shall be interpreted accordingly).
Authorised Subscriber	means an individual or organization which complies with the procedures of the SS1SP PKI RAPP as set out in Annex E of this Policy and is duly authorised by the SS1SPCA to submit a Certificate Signing Request.
Back-Up	means, in relation to Data which is held on any SS1SPCA System, the storage of a copy of that Data for the purpose of ensuring that the copy may be used (if required) to restore or replace the original Data; and "Backed-Up" is to be interpreted accordingly.

Certificate	means either a SS1SP End Entity Certificate or a SS1SPCA Certificate.
Certificate Profile	means a table bearing that title in Annex B and specifying certain parameters to be contained within a Certificate.
Certificate Re-Key	means a change to the Public Key contained within a Certificate bearing a particular serial number which results in a new Certificate being issued.
Certificate Signing Request	means a request for a Certificate submitted by an Eligible Subscriber in accordance with the SS1SP PKI RAPP as set out in Annex E of this Policy.
Cryptographic Module	See Security Container.
Cryptographic Processing	means the generation, storage or use of any Secret Key Material.
Data	means any information, data, knowledge, figures, methodologies, minutes, reports, forecasts, images or sounds (together with any database made up of any of these) embodied in any medium (whether tangible or electronic).
Eligible Subscriber	means: a) in relation to a SS1SP End Entity Certificate, an Authorised Subscriber which is identified as an Eligible Subscriber in accordance with the SS1SP PKI RAPP as set out in Annex E of this Policy; and b) in relation to a SS1SPCA Certificate, an Authorised Subscriber which is identified as an Eligible Subscriber in accordance with the SS1SP PKI RAPP as set out in Annex E of this Policy.

Intermediate Secure S1SP Certification Authority (or Intermediate SS1SPCA)	means the Secure S1SP exercising the function of the Intermediate SS1SPCA to Issue Certificates to Subordinate SS1SPCAs and of storing and managing the Private Keys associated with that function. Intermediate SS1SPCAs comprise the following: a) Operations CA; and b) Manufacturing CA.
Intermediate SS1SPCA Certificate	means a certificate in the form set out in the Intermediate SS1SPCACertificate Profile in accordance with Annex B and Issued by the Root SS1SPCA to the Intermediate SS1SPCA in accordance with this Policy.
Intermediate SS1SPCA Private Key	means a Private Key which is stored and managed by the SS1SPCA acting in its capacity as the Intermediate SS1SPCA.
Key Escrow	means the storage of a Private Key by a person other than the Subscriber or Subject of the Certificate which contains the related Public Key.
Object Identifier (or **OID**)	means an Object Identifier assigned by the Internet Address Naming Authority.
Policy	means this Secure S1SP Certificate Policy.
Private Key	means the private part of an asymmetric Key Pair used for the purposes of public key cryptography
Private Key Material	in relation to a Private Key, means that Private Key and the input parameters necessary to establish, use and maintain it.
Privileged User	means a member of SS1SPCA Personnel who is authorised to carry out activities which involve access to resources, or Data held, on the SS1SPCA System and which are capable of being a means by which the SS1SPCA System, any other Systems, or Secure SMETS1 Device are (or are capable of being) being compromised to a material extent.

Public Key	means the public part of an asymmetric Key Pair used for the purposes of public key cryptography.
Registration Authority	means the Secure S1SP exercising the function of receiving and processing Certificate Signing Requests made in accordance with Annex E: SS1SP PKI RAPP of this Policy.
Registration Authority Manager	means either a director of the Secure S1SP or any other person who may be identified as such in accordance with Annex E: SSS1SP PKI RAPP of this Policy.
Registration Authority Personnel	means those persons who are engaged by the Secure S1SP, in so far as such persons carry out, or are authorised to carry out, any function of the SS1SPCA Registration Authority.
Relying Party	means a SS1SP Party who, pursuant to this Policy, receives and relies upon a Certificate.
Root SS1SP Certification Authority (or **Root SS1SPCA**)	means the Secure S1SP exercising the function of Root SS1SPCA to Issue Certificates to the Intermediate SS1SPCA and storing and managing Private Keys associated with that function.
Root SS1SPCA Certificate	means a certificate in the form set out in the Root SS1SPCA Certificate Profile in accordance with Annex B and self-signed by the Root SS1SPCA in accordance with this Policy.
Root SS1SPCA Private Key	means a Private Key which is stored and managed by the SS1SPCA acting in its capacity as the Root SS1SPCA.
Secret Key Material	means any Private Key, Shared Secret, Symmetric Key or other functionally equivalent cryptographic material (and any associated input parameter) that is generated and maintained by the SS1SPCA.

Secure SMETS1 Service Provider (or SS1SP)	means Secure Meters (UK) Limited (Company number: 02199653).

Secure S1SP Certification Authority (or SS1SPCA)	means the Secure S1SP, acting in the capacity and exercising the functions of one or more of the:
	(a) Root SS1SPCA;
	(b) Intermediate SS1SPCA;
	(c) Subordinate SS1SPCA;
	(d) SS1SPCA Systems; and
	(e) the SS1SP PKI Registration Authority.

Secure SMETS1 Device	means one of the following devices manufactured and provided by Secure:
	a SMETS1 ESME;
	a SMETS1 GSME;
	a SMETS1 CHF;
	a SMETS1 GPF;
	a SMETS1 PPMID;
	a SMETS1 IHD; and
	any other device operating on a home area network created by a SMETS1 CHF.

Secure SMETS1 Service Provider End Entity Certificate (or SS1SP End Entity Certificate)	means a Certificate only issued by one of the Subordinate SS1SPCAs. SS1SP End Entity Certificates comprise the following: a) SMSO TLS Certificate b) SMSO KMS Certificate c) Code Signing Certificate d) Device Certificate
Secure SMETS1 Service Provider PKI (or SS1SP PKI)	means the SS1SPCA System and any public key infrastructure established (or to be established) by Secure for the purpose, among other things, of providing secure communications between Secure S1SP, the DCC and Secure SMETS1 Devices.
Security Container	means a set of hardware, software and/or firmware.

Security Related Functionality	means the functionality of the SS1SPCA Systems which is designed to detect, prevent or mitigate the adverse effect of any security compromise of that System.
Security Sub-Committee or SSC	means the Security Sub-Committee under the Smart Energy Code.
Smart Energy Code	means the code of that name maintained pursuant to the smart meter communication licences granted under the UK Gas Act 1986 and the UK Electricity Act 1989.
SMETS1	means the Smart Metering Equipment Technical Specifications 1.
SSCPKI	means the Security Sub-Committee when performing its PKI functions.
SS1SPCA CSR Generation Tool	means the part of the SS1SPCA System responsible for creating Certificate Requests and validating Certificate Requests.
SS1SPCA Key	means any Private Key or a Public Key generated by the SS1SPCA for the purposes of complying with its obligations under this Policy.
SS1SPCA Management Tool	means the part of the SS1SPCA System responsible for creating and Issuing Certificates.
SS1SPCA Personnel	means those persons who are engaged by the Secure S1SP, in so far as such persons carry out, or are authorised to carry out, any function of the SS1SPCA.
SS1SPCA Public Key	means the Public Key which is part of a Key Pair of a Root SS1SPCA Private Key, an Intermediate SS1SPCA Private Key or a Subordinate SS1SPCA Private Key.
SS1SPCA Private Key	means a SS1SPCA Key which is a Private Key.
SS1SPCA Systems	means the Systems used by the SS1SPCA in relation to the SS1SP PKI services.
SS1SPCA Certificate	means either a Root SS1SPCA Certificate, an Intermediate SS1SPCA Certificate or a Subordinate SS1SPCA Certificate.

SS1SP CPS	means the Certification Practice Statement describing how the PKI is operated and maintained.
SS1SP End Entity Certificate	means a certificate in the form set out in the SS1SP End Entity Certificate Profile in accordance with Annex B of this Policy and Issued by the Subordinate SS1SPCA.
SS1SP Party	means, Secure Meters UK Limited including where they act in this capacity through an individual engaged to act on their behalf or through the use of a System or Secure SMETS1 Device that is the Subject of a Certificate in accordance with this Policy.
SS1SP PKI RAPP	Means the Secure SMETS1 Service Provider Public Key Infrastructure Registration Authority Policy and Procedures as set out in Annex E of this Policy.
Subject	means: (a) in relation to a SS1SP End Entity Certificate, the subject identified by the population of the subject field of the relevant SS1SP End Entity Certificate Profile in Annex B of this Policy; and (b) in relation to a SS1SPCA Certificate, the Root SS1SPCA, Intermediate SS1SPCA or Subordinate SS1SPCA as identified by the subject field of the relevant Certificate Profile in Annex B of this Policy.
Subordinate Secure S1SP Certification Authority (or Subordinate SS1SPCA)	means the Secure S1SP exercising the function of the Subordinate SS1SPCA to Issue SS1SP End Entity Certificates to Eligible Subscribers and of storing and managing the Private Keys associated with that function. Subordinate SS1SPCAs comprise the following: a) SMSO CA b) SMSO KMS CA c) Code Signing CA d) Device CA

Subordinate SS1SPCA Certificate	means a certificate in the form set out in the Subordinate SS1SPCA Certificate Profile in accordance with Annex B and Issued by the Intermediate SS1SPCA to the Subordinate SS1SPCA in accordance with this Policy.
Subordinate SS1SPCA Private Key	means a Private Key which is stored and managed by the SS1SPCA acting in its capacity as the Subordinate SS1SPCA.
Subscriber	means, in relation to any Certificate, an individual, organisation, System or Secure SMETS1 Device which has been Issued with and accepted that Certificate, acting in its capacity as the holder of the Certificate.
System	means a system for generating, sending, receiving, storing (including for the purposes of Back-Up), manipulating or otherwise processing electronic communications, including all hardware, software, firmware and Data associated therewith. This includes the SS1SP PKI System.
Time-Stamping	means the act that takes place when a Time-Stamping Authority, in relation to a Certificate, stamps a particular datum with an accurate indicator of the time (in hours, minutes and seconds) at which the activity of stamping takes place.
Validity Period	means, in respect of a Certificate, the period of time for which that Certificate is intended to be valid.

11 Annex B: SS1SPCA Certificate and SS1SP End entity certificate profiles

11.1 Certificate Structure and Contents

This Annex lays out requirements as to structure and content with which SS1SPCA Certificates and SS1SP End Entity Certificates shall comply. All terms in this Annex shall, where not defined in this Policy, or the GB Companion Specification (GBCS), have the meanings in IETF RFC 5759 or IETF RFC5280.

11.2 Common requirements applicable to SS1SPCA Certificates and SS1SP End Entity Certificates

All SS1SPCA Certificates and SS1SP End Entity Certificates that are validly authorised within the SS1SP PKI for use within the scope of GB Smart Metering:

- shall be compliant with IETF RFC 5759 and so with IETF RFC5280.
- for clarity and in adherence with the requirements of IETF RFC5759, all SS1SPCA Certificates and SS1SP End Entity Certificates shall:
    - contain the `authorityKeyIdentifier` in the form `[0] KeyIdentifier` which shall be marked as non-critical, except where the Certificate is the SS1SPCARoot, in which case `authorityKeyIdentifier` may be omitted;
    - contain the `keyUsage` extension which shall be marked as critical;
    - be X.509 v3 certificates as defined in IETF RFC 5280, encoded using the ASN.1 Distinguished Encoding Rules;
    - only contain Public Keys of types that are explicitly allowed by the Great Britain Companion Specification (GBCS)[1]. This means all Public Keys shall be elliptic curve Public Keys on the NIST P-256 curve;
    - only contain Public Keys in uncompressed form i.e. contain an elliptic curve point in uncompressed form as detailed in Section 2.2 of IETF RFC5480;
    - only provide for signature methods that are explicitly allowed within the GBCS. This means using P-256 Private Keys with SHA 256 and ECDSA;
    - contain a serialNumber which is a positive integer;
    - contain a subjectKeyIdentifier which shall be marked as non-critical;

[1] The latest version of the GBCS can be found here: https://smartenergycodecompany.co.uk/the-smart-energy-code-2/

    - only contain KeyIdentifiers generated as per method (2) of Section 4.2.1.2 of IETF RFC 5280 and so which shall always be 8 octets in length;
    - contain an issuer field whose contents MUST be identical to the contents of the signer's subject field in the signer's Certificate;
    - have a valid notBefore field consisting of the time of issue encoded;
    - other than the S1SP End Entity SMSO TLS and SMSO KMS Certificates, have a valid notAfter field for a not well-defined expiration date as per IETF RFC 5280 Section 4.1.2.5 (so the notAfter shall be assigned the GeneralizedTime value of 99991231235959Z).

11.3 Common Requirements applicable to SS1SP End Entity Certificates only

All SS1SP End Entity Certificates that are issued by the SS1SPCA shall:

- other than the S1SP End Entity SMSO TLS and SMSO KMS Certificates, not have a well-defined expiration date and so the `notAfter` shall be assigned the `GeneralizedTime` value of 99991231235959Z;
- have a `subject` field populated in accordance with each specific SS1SP End Entity Certificate Profile;
- contain a single Public Key;
- SS1SP End Entity Certificates shall contain the extensions described below:
    - `subjectAltName`
    - `keyUsage`
    - `authorityKeyIdentifier`
    - `subjectKeyIdentifier`
- contain a keyUsage extension marked as critical, with a value of one or more of:
    - `digitalSignature`;
    - `keyAgreement`;
    - `nonRepudiation`
    - `keyEncipherment`
    - `dataEncipherment`
- SS1SP End Entity Certificates may contain the `ExtKeyUsage` extension, with a value of one or more of:
    - `id-kp-serverAuth`
    - `id-kp-clientAuth`
    - `id-kp-codeSigning`
- SS1SP End Entity Certificates may contain the `BasicConstraints` extension, with the following values only. `cA` must be FALSE:
    - End Entity

o pathLen=0

11.4 Common Requirements applicable to the Root SS1SPCA, Intermediate SS1SPCA and Subordinate SS1SPCA ONLY

All SS1SPCA Certificates issued by the SS1SPCA shall:

- not have a well-defined expiration date and so the notAfter shall be assigned the GeneralizedTime value of 99991231235959Z;
- must have a Valid notBefore field consisting of the time of issue encoded as per RFC5280;
- Per RFC5280, the IssuerName of any certificates MUST be identical to the signer's subject;
- have a globally unique subject;
- contain a single Public Key;
- contain a keyUsage extension marked as critical and defined as keyCertSign and cRLSign;
- For the Intermediate SS1SPCA Certificates, contain the basicConstraints extension, with values cA=True, and pathLen=1. This extension shall be marked as critical.
- For the Subordinate SS1SPCA Certificates, contain the basicConstraints extension, with values cA=True, and pathLen=0. This extension shall be marked as critical.
- For the Root SS1SPCACertificate, contain the basicConstraints extension, with the value cA=True and pathLen absent (unlimited). This extension shall be marked as critical.
- must create SerialNumbers that are unique and non-negative.

11.5 SS1SP End Entity Certificate Profile - SMSO TLS Certificate

Field Name	RFC 5759/5280 Type	Value	Reference
version	INTEGER	v3	
serialNumber	INTEGER	Positive Integer	
signature	AlgorithmIdentifier	SHA256 with ECDSA	
The value field of the AttributeTypeAndValue structure within the subject field whose type is id-at-commonName (the “Issuer X520 Common Name”)	UTF8String	Globally unique common name of Subordinate SS1SPCA (as defined in the Subordinate SS1SPCA Certificate Profile)	
keyIdentifier in Authoritykeyidentifier (the "Authority Key Identifier")	keyIdentifier	A unique value that matches the subjectKeyIdentifier value of the issuer’s credential	
keyIdentifier in SubjectKeyIdentifier (the "Subject Key Identifier")	keyIdentifier	Provides a means for identifying certificates containing the particular Public Key used in an application	
notBefore	Time	Creation time of the SS1SP End Entity Certificate	

notAfter	Time	shall be assigned the GeneralizedTime value of 5 years from the notBefore Time	
The value field of the AttributeTypeAndValue structure within the subject field whose type is id-at-commonName (the “Subject X520 Common Name”)	UTF8String	Common Name of SS1SP End Entity Certificate	
Key Usage	keyUsage	The permitted Key Usages.	
Enhanced Key Usage	ExtKeyUsage	The permitted Enhanced Key Usages.	
Basic Constraints	BasicConstraints	The permitted Basic Constraints values.	
subjectPublicKeyInfo	SubjectPublicKeyInfo	The Subject’s Public Key	
signatureAlgorithm	AlgorithmIdentifier	SHA256 with ECDSA	
signatureValue	BIT STRING	SS1SP End Entity Certificate signature value	

Interpretation

Version

The version of the X.509 SS1SP End Entity Certificate. Valid SS1SP End Entity Certificates shall identify themselves as version 3.

Serial Number

SS1SP End Entity Certificate serial number, which is a positive integer. The `serialNumber` identifies the SS1SP End Entity Certificate and shall be created by the Subordinate SS1SPCA that signs the SS1SP End Entity Certificate. The `serialNumber` shall be unique in the scope of SS1SP End Entity Certificates signed by the Subordinate SS1SPCA.

Signature

The identity of the signature algorithm used to sign the SS1SP End Entity Certificate. The field is identical to the value of the SS1SP End Entity Certificate `signatureAlgorithm` field explained further under the next **`signatureAlgorithm`** heading below.

Issuer X520 Common Name

The name of the signer of the SS1SP End Entity Certificate. This will be the globally unique name of the Subordinate SS1SPCA (as defined in the Subordinate SS1SPCA Certificate Profile).

Authority Key Identifier

To optimise building the correct credential chain, the non-critical Authority Key Identifier extension shall be populated with a unique value as recommended by RFC 5280 and shall be included in all SS1SP End Entity Certificates.

Subject Key Identifier

The Subject Key Identifier extension should be included and marked as non-critical in the SS1SP End Entity Certificate.

Validity

The time period over which the Subordinate SS1SPCA expects the SS1SP End Entity Certificate to be valid. The `validity` period is the period of time from `notBefore` through `notAfter`, inclusive.

The SMSO TLS End Entity Certificates are valid to operate for 5 years from date of creation.

All times shall be stated in the Universal Coordinated Time (UTC) time zone. Times up to and including 23:59:59 December 31, 2049 UTC shall be encoded as `UTCTime` as YYMMDDHHmmssZ.

Times later than 23:59:59 December 31, 2049 UTC shall be encoded as `GeneralizedTime` as YYYYMMDDHHmmssZ.

Not Before Date

The earliest time a SS1SP End Entity Certificate may be used. This shall be the time the SS1SP End Entity Certificate is created.

Not After Date

The latest time a SS1SP End Entity Certificate is expected to be used. The SMSO TLS End Entity Certificate are valid for 5 years from date of creation.

Subject X520 Common Name

This field must be populated as follows:

```
C = GB
S = Hampshire
L = Winchester
OU = Secure Meters (UK) Ltd
O = Secure Meters (UK) Ltd
CN = s1t.smartwse.net
```

Key Usage

The `keyUsage` extension should be populated as follows:

`digitalSignature`; and

`keyAgreement`.

Enhanced Key Usage

The `ExtKeyUsage` extension should be populated as follows:

`id-kp-serverAuth;` and
`id-kp-clientAuth.`

Basic Constraints

The `BasicConstraints` extension should be populated as follows:

```
cA=False

End Entity

pathLen=0
```

Subject Public Key Info

The SS1SP End Entity Certificate `subjectPublicKeyInfo` field shall indicate the Public Key algorithm identifier and the Public Key in the specified algorithm format as specified in RFC 3279 and RFC 5480.

The algorithm field in the `subjectPublicKeyInfo` structure shall contain the following

identifier:

```
id-ecPublicKey OBJECT IDENTIFIER ::= {iso(1) member-body(2)
us(840) ansi-X9-62(10045) keyType(2) 1 }
```

id-ecPublicKey indicates that the algorithms that can be used with the subject Public Key are unrestricted. The key is only restricted by the values indicated in the `KeyUsage` SS1SP End Entity Certificate extension (explained further under the next **`extensions`** heading below).

The parameter for `id-ecPublicKey` is as follows and shall always be present:

```
    ECParameters ::= CHOICE {
namedCurve         OBJECT IDENTIFIER        -
- implicitCurve   NULL
          -- specifiedCurve  SpecifiedECDomain
      }
```

Only the following field in ECParameters shall be used:

`o namedCurve` - identifies all the required values for a particular set of elliptic curve domain parameters to be represented by an object identifier.

The `OBJECT IDENTIFIER` for the curve choice to be used in SS1SP End Entity Certificate is:

```
secp256r1 OBJECT IDENTIFIER ::= { iso(1) member-body(2) us(840)
ansi-X9-62(10045) curves(3) prime(1) 7 }
```

The `subjectPublicKey` from `SubjectPublicKeyInfo` is the ECC Public Key.

Implementations of Elliptic Curve Cryptography according to this document shall only support the uncompressed form.

The first octet of the `subjectPublicKey` indicates whether the key is compressed or uncompressed. The uncompressed form is indicated by 0x04 (the compressed form is indicated by either 0x02 or 0x03). The Public Key shall be rejected if any value other than 0x04 is in the first octet.

Signature Algorithm

The `signatureAlgorithm` field shall indicate the SS1SPCAIssuing SS1SPCA signature algorithm used to sign this SS1SP End Entity Certificate is as defined under the next **Signature Method (ECDSA)** heading.

Signature Value

The Subordinate SS1SPCA's signature of the SS1SP End Entity Certificate shall be computed using the Subordinate's private signing key using the algorithm identified under the next **Signature Method (ECDSA)** heading.

The structure for ECDSA signatures shall be as per RFC 5480.

Cryptographic Primitives for Signature Method

Signature Method (ECDSA)

The ECDSA signature method is defined in NIST FIPS 186-4. When implementing ECDSA, the SHA-256 message digest algorithm and the P-256 elliptic curve as defined in FIPS 186-4 Annex D, D.1.2.3, shall be used.

The signature algorithm shall be `ecdsa-with-SHA256` as specified in RFC 5759 and 6318.

The algorithm identifier is:

```
ecdsa-with-SHA256 OBJECT IDENTIFIER ::= { iso(1) memberbody(2)
us(840) ansi-X9-62(10045) signatures(4) ecdsa-withsha2(3) 2 }
```

SHA-256 hash algorithm

The hash algorithm used shall be the SHA-256 secure hash algorithm as defined in NIST FIPS 180-4.

11.6 SS1SP End Entity Certificate Profile - SMSO KMS Certificate

Field Name	RFC 5759/5280 Type	Value	Reference
version	INTEGER	v3	
serialNumber	INTEGER	Positive Integer	
signature	AlgorithmIdentifier	SHA256 with ECDSA	
The value field of the AttributeTypeAndValue structure within the subject field whose type is id-at-commonName (the "Issuer X520 Common Name")	UTF8String	Globally unique common name of Subordinate SS1SPCA (as defined in the Subordinate SS1SPCA Certificate Profile)	

keyIdentifier in Authoritykeyidentifier (the "Authority Key Identifier")	keyIdentifier	A unique value that matches the subjectKeyIdentifier value of the issuer’s credential	
keyIdentifier in SubjectKeyIdentifier (the "Subject Key Identifier")	keyIdentifier	Provides a means for identifying certificates containing the particular Public Key used in an application	
notBefore	Time	Creation time of the SS1SP End Entity Certificate	
notAfter	Time	shall be assigned the GeneralizedTime value of 5 years from the notBefore Time	
The value field of the AttributeTypeAndValue structure within the subject field whose type is id-at-commonName (the “Subject X520 Common Name”)	UTF8String	Common Name of SS1SP End Entity	
Key Usage	keyUsage	The permitted Key Usages.	

Basic Constraints	`BasicConstraints`	The permitted Basic Constraints values.	
`subjectPublicKeyInfo`	`SubjectPublicKeyInfo`	The Subject's Public Key	
`signatureAlgorithm`	`AlgorithmIdentifier`	SHA256 with ECDSA	
`signatureValue`	`BIT STRING`	SS1SP End Entity Certificate signature value	

Interpretation

Version

The version of the X.509 SS1SP End Entity Certificate. Valid SS1SP End Entity Certificates shall identify themselves as version 3.

Serial Number

SS1SP End Entity Certificate serial number, which is a positive integer. The `serialNumber` identifies the SS1SP End Entity Certificate and shall be created by the Subordinate SS1SPCA that signs the SS1SP End Entity Certificate. The `serialNumber` shall be unique in the scope of SS1SP End Entity Certificates signed by the Subordinate SS1SPCA.

Signature

The identity of the signature algorithm used to sign the SS1SP End Entity Certificate. The field is identical to the value of the SS1SP End Entity Certificate `signatureAlgorithm` field explained further under the next **`signatureAlgorithm`** heading below.

Issuer X520 Common Name

The name of the signer of the SS1SP End Entity Certificate. This will be the globally unique name of the Subordinate SS1SPCA (as defined in the Subordinate SS1SPCA Certificate Profile).

Authority Key Identifier

To optimise building the correct credential chain, the non-critical Authority Key Identifier extension shall be populated with a unique value as recommended by RFC 5280 and shall be included in all SS1SP End Entity Certificates.

Subject Key Identifier

The Subject Key Identifier extension should be included and marked as non-critical in the SS1SP End Entity Certificate.

Validity

The time period over which the Subordinate SS1SPCA expects the SS1SP End Entity Certificate to be valid. The `validity` period is the period of time from `notBefore` through `notAfter`, inclusive.

The SMSO KMS End Entity Certificates is valid to operate for 5 years from date of creation.

All times shall be stated in the Universal Coordinated Time (UTC) time zone. Times up to and including 23:59:59 December 31, 2049 UTC shall be encoded as `UTCTime` as YYMMDDHHmmssZ.

Times later than 23:59:59 December 31, 2049 UTC shall be encoded as `GeneralizedTime` as YYYYMMDDHHmmssZ.

Not Before Date

The earliest time a SS1SP End Entity Certificate may be used. This shall be the time the SS1SP End Entity Certificate is created.

Not After Date

The latest time a SS1SP End Entity Certificate is expected to be used. The SMSO KMS End Entity Certificate is valid for 5 years from date of creation.

Subject X520 Common Name

This field must be populated as follows:

```
C = [Country]
S = [County]
L = [Location/City]
OU = [Supplier's Organisational Unit]
O = [Supplier's Organisation Name]
CN = [Supplier's Trading Name]
```

Key Usage

The `keyUsage` extension should be populated as follows:

`digitalSignature`; and

`keyAgreement`.

Basic Constraints

The `BasicConstraints` extension should be populated as follows:

```
cA=False

End Entity

pathLen=0
```

Subject Public Key Info

The SS1SP End Entity Certificate `subjectPublicKeyInfo` field shall indicate the Public Key algorithm identifier and the Public Key in the specified algorithm format as specified in RFC 3279 and RFC 5480.

The algorithm field in the `subjectPublicKeyInfo` structure shall contain the following

identifier:

```
        id-ecPublicKey OBJECT IDENTIFIER ::= {iso(1) member-body(2)
        us(840) ansi-X9-62(10045) keyType(2) 1 }
```

id-ecPublicKey indicates that the algorithms that can be used with the subject Public Key are unrestricted. The key is only restricted by the values indicated in the `KeyUsage` SS1SP End Entity Certificate extension (explained further under the next **`extensions`** heading below).

The parameter for `id-ecPublicKey` is as follows and shall always be present:

```
            ECParameters ::= CHOICE {

        namedCurve         OBJECT IDENTIFIER        -

        - implicitCurve   NULL
```

```
            -- specifiedCurve  SpecifiedECDomain
         }
```

Only the following field in ECParameters shall be used:

o `namedCurve` - identifies all the required values for a particular set of elliptic curve domain parameters to be represented by an object identifier.

The `OBJECT IDENTIFIER` for the curve choice to be used in SS1SP End Entity Certificate is:

```
secp256r1 OBJECT IDENTIFIER ::= { iso(1) member-body(2) us(840)
ansi-X9-62(10045) curves(3) prime(1) 7 }
```

The `subjectPublicKey` from `SubjectPublicKeyInfo` is the ECC Public Key.

Implementations of Elliptic Curve Cryptography according to this document shall only support the uncompressed form.

The first octet of the `subjectPublicKey` indicates whether the key is compressed or uncompressed. The uncompressed form is indicated by 0x04 (the compressed form is indicated by either 0x02 or 0x03). The Public Key shall be rejected if any value other than 0x04 is in the first octet.

Signature Algorithm

The `signatureAlgorithm` field shall indicate the Subordinate SS1SPCA signature algorithm used to sign this SS1SP End Entity Certificate is as defined under the next **Signature Method (ECDSA)** heading.

Signature Value

The Subordinate SS1SPCA's signature of the SS1SP End Entity Certificate shall be computed using the Subordinate SS1SPCA's private signing key using the algorithm identified under the next **Signature Method (ECDSA)** heading.

The structure for ECDSA signatures shall be as per RFC 5480.

Cryptographic Primitives for Signature Method

Signature Method (ECDSA)

The ECDSA signature method is defined in NIST FIPS 186-4. When implementing ECDSA, the SHA-256 message digest algorithm and the P-256 elliptic curve as defined in FIPS 186-4 Annex D, D.1.2.3, shall be used.

The signature algorithm shall be `ecdsa-with-SHA256` as specified in RFC 5759 and 6318.

The algorithm identifier is:

```
ecdsa-with-SHA256 OBJECT IDENTIFIER ::= { iso(1) memberbody(2)
us(840) ansi-X9-62(10045) signatures(4) ecdsa-withsha2(3) 2 }
```

SHA-256 hash algorithm

The hash algorithm used shall be the SHA-256 secure hash algorithm as defined in NIST FIPS 180-4.

11.7 SS1SP End Entity Certificate Profile - Code Signing Certificate

Field Name	RFC 5759/5280 Type	Value	Reference

version	INTEGER	v3	
serialNumber	INTEGER	Positive Integer	
signature	AlgorithmIdentifier	SHA256 with ECDSA	
The value field of the AttributeTypeAndValue structure within the subject field whose type is id-at-commonName (the "Issuer X520 Common Name")	UTF8String	Globally unique common name of Subordinate SS1SPCA (as defined in the Subordinate SS1SPCA Certificate Profile)	
keyIdentifier in Authoritykeyidentifier (the "Authority Key Identifier")	keyIdentifier	A unique value that matches the subjectKeyIdentifier value of the issuer's credential	
keyIdentifier in SubjectKeyIdentifier (the "Subject Key Identifier")	keyIdentifier	Provides a means for identifying certificates containing the particular Public Key used in an application	
notBefore	Time	Creation time of the SS1SP End Entity Certificate	

notAfter	Time	shall be assigned the GeneralizedTime value of 99991231235959Z	
The value field of the AttributeTypeAndValue structure within the subject field whose type is id-at-commonName (the “Subject X520 Common Name”)	UTF8String	Common Name of SS1SP End Entity	
Key Usage	keyUsage	The permitted Key Usages.	
Enhanced Key Usage	ExtKeyUsage	The permitted Enhanced Key Usages.	
Basic Constraints	BasicConstraints	The permitted Basic Constraints values.	
subjectPublicKeyInfo	SubjectPublicKeyInfo	The Subject’s Public Key	
signatureAlgorithm	AlgorithmIdentifier	SHA256 with ECDSA	
signatureValue	BIT STRING	SS1SP End Entity Certificate signature value	

Interpretation

Version

The version of the X.509 SS1SP End Entity Certificate. Valid SS1SP End Entity Certificates shall identify themselves as version 3.

Serial Number

SS1SP End Entity Certificate serial number, which is a positive integer. The `serialNumber` identifies the SS1SP End Entity Certificate and shall be created by the Subordinate SS1SPCA that signs the SS1SP End Entity Certificate. The `serialNumber` shall be unique in the scope of SS1SP End Entity Certificates signed by the Subordinate SS1SPCA.

Signature

The identity of the signature algorithm used to sign the SS1SP End Entity Certificate. The field is identical to the value of the SS1SP End Entity Certificate `signatureAlgorithm` field explained further under the next **`signatureAlgorithm`** heading below.

Issuer X520 Common Name

The name of the signer of the SS1SP End Entity Certificate. This will be the globally unique name of the Subordinate SS1SPCA (as defined in the Subordinate SS1SPCA Certificate Profile).

Authority Key Identifier

To optimise building the correct credential chain, the non-critical Authority Key Identifier extension shall be populated with a unique value as recommended by RFC 5280 and shall be included in all SS1SP End Entity Certificates.

Subject Key Identifier

The Subject Key Identifier extension should be included and marked as non-critical in the SS1SP End Entity Certificate.

Validity

The time period over which the Subordinate SS1SPCA expects the SS1SP End Entity Certificate to be valid. The `validity` period is the period of time from `notBefore` through `notAfter`, inclusive.

All times shall be stated in the Universal Coordinated Time (UTC) time zone. Times up to and including 23:59:59 December 31, 2049 UTC shall be encoded as `UTCTime` as YYMMDDHHmmssZ.

Times later than 23:59:59 December 31, 2049 UTC shall be encoded as `GeneralizedTime` as YYYYMMDDHHmmssZ.

Not Before Date

The earliest time a SS1SP End Entity Certificate may be used. This shall be the time the SS1SP End Entity Certificate is created.

Not After Date

The latest time a Certificate is expected to be used (`notAfter`). Code Signing End Entity Certificates are expected to operate indefinitely into the future and should use the value `99991231235959Z`. Systems or Secure SMETS1 Devices verifying a Certificate are expected to accept this value indefinitely.

Subject X520 Common Name

This field must be populated as follows:

C = IN

S = Rajasthan

L = Udaipur

OU = Secure Meters Ltd

O = Secure Meters Ltd

CN = Secure Meters Firmware Signer

Key Usage

The keyUsage extension should be populated as follows:

digitalSignature; and

nonRepudiation.

Enhanced Key Usage

The ExtKeyUsage extension should be populated as follows:

id-kp-codeSigning

Basic Constraints

The BasicConstraints extension should be populated as follows:

cA=False

End Entity

pathLen=0

Subject Public Key Info

The SS1SP End Entity Certificate `subjectPublicKeyInfo` field shall indicate the Public Key algorithm identifier and the Public Key in the specified algorithm format as specified in RFC 3279 and RFC 5480.

The algorithm field in the `subjectPublicKeyInfo` structure shall contain the following identifier:

```
id-ecPublicKey OBJECT IDENTIFIER ::= {iso(1) member-body(2)
us(840) ansi-X9-62(10045) keyType(2) 1 }
```

id-ecPublicKey indicates that the algorithms that can be used with the subject Public Key are unrestricted. The key is only restricted by the values indicated in the `KeyUsage` SS1SP End Entity Certificate extension (explained further under the next **`extensions`** heading below).

The parameter for `id-ecPublicKey` is as follows and shall always be present:

```
    ECParameters ::= CHOICE {
namedCurve         OBJECT IDENTIFIER        -
- implicitCurve   NULL
       -- specifiedCurve  SpecifiedECDomain
      }
```

Only the following field in ECParameters shall be used:

o `namedCurve` - identifies all the required values for a particular set of elliptic curve domain parameters to be represented by an object identifier.

The `OBJECT IDENTIFIER` for the curve choice to be used in SS1SP End Entity Certificate is:

```
secp256r1 OBJECT IDENTIFIER ::= { iso(1) member-body(2) us(840)
ansi-X9-62(10045) curves(3) prime(1) 7 }
```

The `subjectPublicKey` from `SubjectPublicKeyInfo` is the ECC Public Key.

Implementations of Elliptic Curve Cryptography according to this document shall only support the uncompressed form.

The first octet of the `subjectPublicKey` indicates whether the key is compressed or uncompressed. The uncompressed form is indicated by 0x04 (the compressed form is indicated by either 0x02 or 0x03). The Public Key shall be rejected if any value other than 0x04 is in the first octet.

Signature Algorithm

The `signatureAlgorithm` field shall indicate the Subordinate SS1SPCA signature algorithm used to sign this SS1SP End Entity Certificate is as defined under the next **Signature Method (ECDSA)** heading.

Signature Value

The Subordinate SS1SPCA's signature of the SS1SP End Entity Certificate shall be computed using the Subordinate SS1SPCA's private signing key using the algorithm identified under the next **Signature Method (ECDSA)** heading.

The structure for ECDSA signatures shall be as per RFC 5480.

Cryptographic Primitives for Signature Method

Signature Method (ECDSA)

The ECDSA signature method is defined in NIST FIPS 186-4. When implementing ECDSA, the SHA-256 message digest algorithm and the P-256 elliptic curve as defined in FIPS 186-4 Annex D, D.1.2.3, shall be used.

The signature algorithm shall be `ecdsa-with-SHA256` as specified in RFC 5759 and 6318.

The algorithm identifier is:

```
ecdsa-with-SHA256 OBJECT IDENTIFIER ::= { iso(1) memberbody(2)
us(840) ansi-X9-62(10045) signatures(4) ecdsa-withsha2(3) 2 }
```

SHA-256 hash algorithm

The hash algorithm used shall be the SHA-256 secure hash algorithm as defined in NIST FIPS 180-4.

11.8 SS1SP End Entity Certificate Profile - Device Certificate

Field Name	RFC 5759/5280 Type	Value	Reference
version	INTEGER	v3	
serialNumber	INTEGER	Positive Integer	
signature	AlgorithmIdentifier	SHA256 with ECDSA	
The value field of the AttributeTypeAndValue structure within the subject field whose type is id-at-commonName (the “Issuer X520 Common Name”)	UTF8String	Globally unique common name of Subordinate SS1SPCA (as defined in the Subordinate SS1SPCA Certificate Profile)	

keyIdentifier in Authoritykeyidentifier (the "Authority Key Identifier")	keyIdentifier	A unique value that matches the subjectKeyIdentifier value of the issuer's credential	
keyIdentifier in SubjectKeyIdentifier (the "Subject Key Identifier")	keyIdentifier	Provides a means for identifying certificates containing the particular Public Key used in an application	
notBefore	Time	Creation time of the SS1SP End Entity Certificate	
notAfter	Time	shall be assigned the GeneralizedTime value of 99991231235959Z	
The value field of the AttributeTypeAndValue structure within the subject field whose type is id-at-commonName (the "Subject X520 Common Name")	UTF8String	Common Name of SS1SP End Entity	
Key Usage	keyUsage	The permitted Key Usages.	

Enhanced Key Usage	ExtKeyUsage	The permitted Enhanced Key Usages.	
Basic Constraints	BasicConstraints	The permitted Basic Constraints values.	
subjectPublicKeyInfo	SubjectPublicKeyInfo	The Subject’s Public Key	
signatureAlgorithm	AlgorithmIdentifier	SHA256 with ECDSA	
signatureValue	BIT STRING	SS1SP End Entity Certificate signature value	

Interpretation

Version

The version of the X.509 SS1SP End Entity Certificate. Valid SS1SP End Entity Certificates shall identify themselves as version 3.

Serial Number

SS1SP End Entity Certificate serial number, which is a positive integer. The serialNumber identifies the SS1SP End Entity Certificate and shall be created by the Subordinate SS1SPCA that signs the SS1SP End Entity Certificate. The serialNumber shall be unique in the scope of SS1SP End Entity Certificates signed by the Subordinate SS1SPCA.

Signature

The identity of the signature algorithm used to sign the SS1SP End Entity Certificate. The field is identical to the value of the SS1SP End Entity Certificate `signatureAlgorithm` field explained further under the next **`signatureAlgorithm`** heading below.

Issuer X520 Common Name

The name of the signer of the SS1SP End Entity Certificate. This will be the globally unique name of the Subordinate SS1SPCA (as defined in the Subordinate SS1SPCA Certificate Profile).

Authority Key Identifier

To optimise building the correct credential chain, the non-critical Authority Key Identifier extension shall be populated with a unique value as recommended by RFC 5280 and shall be included in all SS1SP End Entity Certificates.

Subject Key Identifier

The Subject Key Identifier extension should be included and marked as non-critical in the SS1SP End Entity Certificate.

Validity

The time period over which the Subordinate SS1SPCA expects the SS1SP End Entity Certificate to be valid. The `validity` period is the period of time from `notBefore` through `notAfter`, inclusive.

All times shall be stated in the Universal Coordinated Time (UTC) time zone. Times up to and including 23:59:59 December 31, 2049 UTC shall be encoded as `UTCTime` as YYMMDDHHmmssZ.

Times later than 23:59:59 December 31, 2049 UTC shall be encoded as `GeneralizedTime` as YYYYMMDDHHmmssZ.

Not Before Date

The earliest time a SS1SP End Entity Certificate may be used. This shall be the time the SS1SP End Entity Certificate is created.

Not After Date

The latest time a Certificate is expected to be used (`notAfter`). Code Signing End Entity Certificates are expected to operate indefinitely into the future and should use the value `99991231235959Z`. Systems or Secure SMETS1 Devices verifying a Certificate are expected to accept this value indefinitely.

Subject X520 Common Name

This field must be populated as follows:

```
SERIALNUMBER = 000000000195BB18
CN = Q0007098
```

Key Usage

The `keyUsage` extension should be populated as follows:

```
digitalSignature;
```

keyAgreement;

nonrepudiation;

keyEncipherment;and

dataEncipherment.

Enhanced Key Usage

The ExtKeyUsage extension should be populated as follows:

id-kp-serverAuth; and

id-kp-clientAuth.

Basic Constraints

The BasicConstraints extension should be populated as follows:

cA=False

End Entity

pathLen=0

Subject Public Key Info

The SS1SP End Entity Certificate subjectPublicKeyInfo field shall indicate the Public Key algorithm identifier and the Public Key in the specified algorithm format as specified in RFC 3279 and RFC 5480.

The algorithm field in the subjectPublicKeyInfo structure shall contain the following identifier:

```
        id-ecPublicKey OBJECT IDENTIFIER ::= {iso(1) member-body(2)
        us(840) ansi-X9-62(10045) keyType(2) 1 }
```

id-ecPublicKey indicates that the algorithms that can be used with the subject Public Key are unrestricted. The key is only restricted by the values indicated in the KeyUsage SS1SP End Entity Certificate extension (explained further under the next **extensions** heading below).

The parameter for id-ecPublicKey is as follows and shall always be present:

```
           ECParameters ::= CHOICE {
       namedCurve         OBJECT IDENTIFIER        -
       - implicitCurve   NULL
              -- specifiedCurve  SpecifiedECDomain
             }
```

Only the following field in ECParameters shall be used:

o namedCurve - identifies all the required values for a particular set of elliptic curve domain parameters to be represented by an object identifier.

The OBJECT IDENTIFIER for the curve choice to be used in SS1SP End Entity Certificate is:

```
secp256r1 OBJECT IDENTIFIER ::= { iso(1) member-body(2) us(840)
ansi-X9-62(10045) curves(3) prime(1) 7 }
```

The subjectPublicKey from SubjectPublicKeyInfo is the ECC Public Key.

Implementations of Elliptic Curve Cryptography according to this document shall only support the uncompressed form.

The first octet of the subjectPublicKey indicates whether the key is compressed or uncompressed. The uncompressed form is indicated by 0x04 (the compressed form is indicated by either 0x02 or 0x03). The Public Key shall be rejected if any value other than 0x04 is in the first octet.

Signature Algorithm

The `signatureAlgorithm` field shall indicate the Subordinate SS1SPCA signature algorithm used to sign this SS1SP End Entity Certificate is as defined under the next **Signature Method (ECDSA)** heading.

Signature Value

The Subordinate SS1SPCA's signature of the SS1SP End Entity Certificate shall be computed using the Subordinate SS1SPCA's private signing key using the algorithm identified under the next **Signature Method (ECDSA)** heading.

The structure for ECDSA signatures shall be as per RFC 5480.

Cryptographic Primitives for Signature Method

Signature Method (ECDSA)

The ECDSA signature method is defined in NIST FIPS 186-4. When implementing ECDSA, the SHA-256 message digest algorithm and the P-256 elliptic curve as defined in FIPS 186-4 Annex D, D.1.2.3, shall be used.

The signature algorithm shall be `ecdsa-with-SHA256` as specified in RFC 5759 and 6318.

The algorithm identifier is:

```
ecdsa-with-SHA256 OBJECT IDENTIFIER ::= { iso(1) memberbody(2)
us(840) ansi-X9-62(10045) signatures(4) ecdsa-withsha2(3) 2 }
```

SHA-256 hash algorithm

The hash algorithm used shall be the SHA-256 secure hash algorithm as defined in NIST FIPS 180-4.

11.9 Root SS1SPCA Certificate Profile

Field Name	RFC 5759/5280 Type	Value	Reference
version	INTEGER	v3	
serialNumber	INTEGER	Positive Integer	
signature	AlgorithmIdentifier	SHA256 with ECDSA	
The value field of the AttributeTypeAndValue structure within the subject field whose type is id-at-commonName (the “Issuer X520 Common Name”)	UTF8String	Globally unique common name of Root SS1SPCA	
keyIdentifier in subjectKeyIdentifier (the "Subject Key Identifider")	keyIdentifier	A unique value that matches the subjectKeyIdentifier of the issuer’s credential	

notBefore	Time	Creation time of the Certificate	
notAfter	Time	shall be assigned the GeneralizedTime value of 99991231235959Z	
The value field of the AttributeTypeAndValue structure within the subject field whose type is id-atcommonName (the “Subject X520 Common Name”)	UTF8String	Globally unique name of Root SS1SPCA (same as Issuer name)	
Key Usage	keyUsage	The permitted Key Usages.	
Basic Constraints	BasicConstraints	The permitted Basic Constraints values.	
subjectPublicKeyInfo	SubjectPublicKey Info	The Subject’s Public Key	
signatureAlgori thm	AlgorithmIdentifier	SHA256 with ECDSA	
signatureValue	BIT STRING	Subject Certificate signature	

These certificates are the root of trust for the Secure S1SP PKI.

Version

The version of the X.509 Certificate. Valid Certificates shall identify themselves as version 3.

Serial Number

Certificate serial number, which is a positive integer. The `serialNumber` identifies the Certificate, and shall be created by the SS1SPCA that signs the Certificate (self-signed by Root SS1SPCA). The `serialNumber` shall be unique in the scope of Certificates signed by the SS1SPCA.

Signature

The identity of the signature algorithm used to sign the Certificate. The field is identical to the value of the Root SS1SPCA Certificate's `signatureAlgorithm` field explained further under the next **Signature Algorithm heading**.

Issuer X520 Common Name

The name of the signer of the Certificate. This will be the globally unique name of the Root SS1SPCA. This will be the same as the `subject` as it is self-signed by the Root SS1SPCA.

Subject Key Identifier

The `subjectKeyIdentifier` extension should be included and marked as non-critical in the Certificate.

Validity

The time period over which the issuer expects the Certificate to be valid. The validity period is the period of time from `notBefore` through `notAfter`, inclusive.

Root SS1SPCA Certificates are expected to operate indefinitely into the future and should use the value 99991231235959Z. Solutions verifying a Root SS1SPCA Certificate are expected to accept this value indefinitely.

All times shall be stated in the Universal Coordinated Time (UTC) time zone. Times up to and including 23:59:59 December 31, 2049 UTC shall be encoded as `UTCTime` as YYMMDDHHmmssZ.

Times later than 23:59:59 December 31, 2049 UTC shall be encoded as `GeneralizedTime` as YYYYMMDDHHmmssZ.

Not Before Date

The earliest time a Certificate may be used (`notBefore`). This shall be the time the Certificate is created.

Not After Date

The latest time a Certificate is expected to be used (`notAfter`). Certificates are expected to operate indefinitely into the future and should use the value 99991231235959Z. Systems or Secure SMETS1 Devices verifying a Certificate are expected to accept this value indefinitely.

Subject X520 Common Name

This field must be populated as follows:

```
C = GB
S = Hampshire
L = Winchester
OU = Secure Meters (UK) Ltd
```

```
O = Secure Meters (UK) Ltd
CN = Secure Meters (UK) Root CA
```

Key Usage

The `keyUsage` extension should be populated as follows:

`keyCertSign`; and

`cRLSign`

Basic Constraints

The `BasicConstraints` extension should be populated as follows:

`cA=TRUE`

`pathLen=Absent`

Subject Public Key Info

The Certificate's `subjectPublicKeyInfo` field shall indicate the Public Key algorithm identifier and the Public Key in the specified algorithm format as specified in RFC 3279 and RFC 5480.

The algorithm field in the `subjectPublicKeyInfo` structure shall be use the following identifier:

id-ecPublicKey OBJECT IDENTIFIER ::= {iso(1) member-body(2) us(840) ansi-X9-62(10045) keyType(2) 1 } `id-ecPublicKey` indicates that the algorithms that can be used with the subject Public Key are unrestricted. The key is only restricted by the values indicated in the Key Usage Certificate extension (explained further under the next **extensions** heading).

The parameter for `id-ecPublicKey` is as follows and shall always be present:

```
    ECParameters ::= CHOICE {
namedCurve          OBJECT IDENTIFIER         -
- implicitCurve   NULL         --
specifiedCurve  SpecifiedECDomain
      }
```

Only the following field in ECParameters shall be used: o

`namedCurve` - identifies all the required values for a particular

set of elliptic curve domain parameters to be represented by an

`OBJECT IDENTIFIER`.

The object identifier for the curve choice to be used in SS1SPCA Certificates is:

```
secp256r1 OBJECT IDENTIFIER ::= { iso(1) member-body(2) us(840)
ansi-X9-62(10045) curves(3) prime(1) 7 }
```

The `subjectPublicKey` from `SubjectPublicKeyInfo` is the ECC Public Key.

Implementations of Elliptic Curve Cryptography according to this document shall only support the uncompressed form.

The first octet of the `subjectPublicKey` indicates whether the key is compressed or uncompressed. The uncompressed form is indicated by 0x04 (the compressed form is indicated by either 0x02 or 0x03). The Public Key shall be rejected if any value other than 0x04 is in the first octet.

Signature Algorithm

The `signatureAlgorithm` field shall indicate the Root SS1SPCA signature algorithm used to sign this Certificate as defined under the next **Signature Method (ECDSA)** heading.

Signature Value

The Root SS1SPCA's signature of the Certificate shall be computed using the Root SS1SPCA's private signing key using the algorithm identified under the next **Signature Method (ECDSA)** heading .

The structure for ECDSA signatures shall be as per RFC 5480.

Cryptographic Primitives for Signature Method

Signature Method (ECDSA)

The ECDSA signature method is defined in NIST FIPS 186-4. When implementing ECDSA, the SHA-256 message digest algorithm and the P-256 elliptic curve as defined in FIPS 186-4 Annex D, D.1.2.3, shall be used.

The signature algorithm shall be `ecdsa-with-SHA256` as specified in RFC 5759 and 6318.

The algorithm identifier is:

```
ecdsa-with-SHA256 OBJECT IDENTIFIER ::= { iso(1) memberbody(2)
us(840) ansi-X9-62(10045) signatures(4) ecdsa-withsha2(3) 2 }
```

SHA-256 hash algorithm

The hash algorithm shall be the SHA-256 secure hash algorithm as defined in NIST FIPS 180-4.

11.10 Intermediate SS1SPCA Certificate Profile - Operations CA

Field Name	RFC 5759/5280 Type	Value	Reference
version	INTEGER	v3	
serialNumber	INTEGER	Positive Integer	
signature	AlgorithmIdentifier	SHA256 with ECDSA	
The value field of the AttributeTypeAndValue structure within the subject field whose type is id-at-commonName (the "Issuer X520 Common Name")	UTF8String	Globally unique name of Root SS1SPCA (as defined in the Root SS1SPCA Certificate Profile)	
keyIdentifier in subjectKeyIdentif ier (the "Subject Key Identifier")	keyIdentifier	Provides a means for identifying certificates containing the particular Public Key used in an application	
keyIdentifier in authorityKeyIdentifier (the "Authority Key Identifier")	keyIdentifier	A unique value that matches the subjectKeyIdentifier value of the issuer's credential	

notBefore	Time	Creation time of the certificate	
notAfter	Time	shall be assigned the GeneralizedTime value of 99991231235959Z	
The value field of the AttributeTypeAndValue structure within the subject field whose type is id-atcommonName (the "Subject X520 Common Name")	UTF8String	Globally unique name of Intermediate SS1SPCA	
Key Usage	keyUsage	The permitted Key Usages.	
Basic Constraints	BasicConstraints	The permitted Basic Constraints values.	
subjectPublicKeyI nfo	SubjectPublicKeyI nfo	The Subject's Public Key	
signatureAlgorithm	AlgorithmIdentifier	SHA256 with ECDSA	
signatureValue	BIT STRING	Subject certificate signature	

Version

The version of the X.509 Certificate. Valid Certificates shall identify themselves as version 3.

Serial Number

Certificate serial number which is a positive integer. The `serialNumber` identifies the Certificate and shall be created by the SS1SPCA that signs the Certificate. The `serialNumber` shall be unique in the scope of Certificates signed by the Root SS1SPCA.

Signature

The identity of the signature algorithm used to sign the Certificate. The field is identical to the value of the Issuing SS1SPCA Certificate's `signatureAlgorithm` field explained further under the next **Signature Algorithm** heading.

Issuer X520 Common Name

The name of the signer of the Certificate. This will be the globally unique name of the Root SS1SPCA (as defined in the Root SS1SPCA Certificate Profile).

Subject Key Identifier

The `subjectKeyIdentifier` extension should be included and marked as non-critical in the Certificate.

Authority Key Identifier

To optimize building the correct credential chain, the non-critical `authorityKeyIdentifier` extension shall be populated with a unique value as recommended by RFC 5280 and shall be included in all SS1SP End Entity Certificates.

Validity

The time period over which the issuer expects the Certificate to be valid. The `validity` period is the period of time from `notBefore` through `notAfter`, inclusive.

Intermediate SS1SPCA Certificates are expected to operate indefinitely into the future and should use the value 99991231235959Z. Solutions verifying a Intermediate SS1SPCA Certificate are expected to accept this value indefinitely.

All times shall be stated in the Universal Coordinated Time (UTC) time zone. Times up to and including 23:59:59 December 31, 2049 UTC shall be encoded as `UTCTime` as

YYMMDDHHmmssZ.

Times later than 23:59:59 December 31, 2049 UTC shall be encoded as `GeneralizedTime` as

YYYYMMDDHHmmssZ.

Not Before Date

The earliest time a Certificate may be used (`notBefore`). This shall be the time the Certificate is created.

Not After Date

The latest time a Certificate is expected to be used (`notAfter`). Certificates are expected to operate indefinitely into the future and should use the value 99991231235959Z. Systems and Secure SMETS1 Devices verifying a Certificate are expected to accept this value indefinitely.

Subject X520 Common Name

This field shall be populated with the following values:

```
C = GB
S = Hampshire
L = Winchester
OU = Secure Meters (UK) Ltd
O = Secure Meters (UK) Ltd
CN = SML-DCC Operations CA
```

Key Usage

The `keyUsage` extension should be populated as follows:

`keyCertSign;` and

`cRLSign`

Basic Constraints

The `BasicConstraints` extension should be populated as follows:

```
cA=TRUE
pathLen=Absent
```

Subject Public Key Info

The Certificate's `subjectPublicKeyInfo` field shall indicate the Public Key algorithm identifier and the Public Key in the specified algorithm format as specified in RFC 3279 and RFC 5480.

The algorithm field in the `subjectPublicKeyInfo` structure shall contain the following identifier:

```
        id-ecPublicKey OBJECT IDENTIFIER ::= {iso(1) member-body(2)
        us(840) ansi-X9-62(10045) keyType(2) 1 }
```

`id-ecPublicKey` indicates that the algorithms that can be used with the subject Public Key are unrestricted. The key is only restricted by the values indicated in the key usage Certificate extension (explained further under the next **extensions** heading).

The parameter for `id-ecPublicKey` is as follows and shall always be present:

```
    ECParameters ::= CHOICE {

namedCurve          OBJECT IDENTIFIER        -

- implicitCurve    NULL         --

specifiedCurve   SpecifiedECDomain

     }
```

Only the following field in ECParameters shall be used: o

`namedCurve` - identifies all the required values for a particular set

of elliptic curve domain parameters to be represented by an

`OBJECT IDENTIFIER`.

The object identifier for the curve choice to be used in Certificates is:

```
        secp256r1 OBJECT IDENTIFIER ::= { iso(1) member-body(2) us(840)
        ansi-X9-62(10045) curves(3) prime(1) 7 }
```

The `subjectPublicKey` from `SubjectPublicKeyInfo` is the ECC Public Key.

Implementations of Elliptic Curve Cryptography according to this document shall only support the uncompressed form.

The first octet of the `subjectPublicKey` indicates whether the key is compressed or uncompressed. The uncompressed form is indicated by 0x04 (the compressed form is indicated by either 0x02 or 0x03). The Public Key MUST be rejected if any value other than 0x04 is included in the first octet.

Signature Algorithm

The `signatureAlgorithm` field shall indicate the Root SS1SPCA signature algorithm used to sign this Certificate as defined under the next **Signature Method (ECDSA)** heading.

Signature Value

The Root SS1SPCA's signature of the Certificate shall be computed using the Root SS1SPCA's private signing key using the algorithm identified under the next **Signature Method (ECDSA)** heading.

The structure for ECDSA signatures shall be as per RFC 5480.

Cryptographic Primitives for Signature Method

Signature Method (ECDSA)

The ECDSA signature method is defined in NIST FIPS 186-4. When implementing ECDSA, the SHA-256 message digest algorithm and the P-256 elliptic curve as defined in FIPS 186-4 Annex D, D.1.2.3, shall be used.

The signature algorithm shall be `ecdsa-with-SHA256` as specified in RFC 5759 and 6318.

The algorithm identifier is:

```
        ecdsa-with-SHA256 OBJECT IDENTIFIER ::= { iso(1) memberbody(2)
        us(840) ansi-X9-62(10045) signatures(4) ecdsa-withsha2(3) 2 }
```

SHA-256 hash algorithm

The hash algorithm used shall be the SHA-256 secure hash algorithm as defined in NIST FIPS 180-4.

11.11 Intermediate SS1SPCA Certificate Profile - Operations CA

Field Name	RFC 5759/5280 Type	Value	Reference
version	INTEGER	v3	
serialNumber	INTEGER	Positive Integer	
signature	AlgorithmIdentifier	SHA256 with ECDSA	
The value field of the AttributeTypeAndValue structure within the subject field whose type is id-at-commonName (the "Issuer X520 Common Name")	UTF8String	Globally unique name of Root SS1SPCA (as defined in the Root SS1SPCA Certificate Profile)	
keyIdentifier in subjectKeyIdentif ier (the "Subject Key Identifier")	keyIdentifier	Provides a means for identifying certificates containing the particular Public Key used in an application	
keyIdentifier in authorityKeyIdentifier (the "Authority Key Identifier")	keyIdentifier	A unique value that matches the subjectKeyIdentifier value of the issuer's credential	

notBefore	Time	Creation time of the certificate	
notAfter	Time	shall be assigned the GeneralizedTime value of 99991231235959Z	
The value field of the AttributeTypeAndValue structure within the subject field whose type is id-atcommonName (the “Subject X520 Common Name”)	UTF8String	Globally unique name of Intermediate SS1SPCA	
Key Usage	keyUsage	The permitted Key Usages.	
Basic Constraints	BasicConstraints	The permitted Basic Constraints values.	
subjectPublicKeyI nfo	SubjectPublicKeyI nfo	The Subject’s Public Key	
signatureAlgorithm	AlgorithmIdentifier	SHA256 with ECDSA	
signatureValue	BIT STRING	Subject certificate signature	

Version

The version of the X.509 Certificate. Valid Certificates shall identify themselves as version 3.

Serial Number

Certificate serial number which is a positive integer. The `serialNumber` identifies the Certificate and shall be created by the SS1SPCA that signs the Certificate. The `serialNumber` shall be unique in the scope of Certificates signed by the Root SS1SPCA.

Signature

The identity of the signature algorithm used to sign the Certificate. The field is identical to the value of the Issuing SS1SPCA Certificate's `signatureAlgorithm` field explained further under the next **Signature Algorithm** heading.

Issuer X520 Common Name

The name of the signer of the Certificate. This will be the globally unique name of the Root SS1SPCA (as defined in the Root SS1SPCA Certificate Profile).

Subject Key Identifier

The `subjectKeyIdentifier` extension should be included and marked as non-critical in the Certificate.

Authority Key Identifier

To optimize building the correct credential chain, the non-critical authorityKeyIdentifier extension shall be populated with a unique value as recommended by RFC 5280 and shall be included in all SS1SP End Entity Certificates.

Validity

The time period over which the issuer expects the Certificate to be valid. The validity period is the period of time from notBefore through notAfter, inclusive.

Intermediate SS1SPCA Certificates are expected to operate indefinitely into the future and should use the value 99991231235959Z. Solutions verifying a Intermediate SS1SPCA Certificate are expected to accept this value indefinitely.

All times shall be stated in the Universal Coordinated Time (UTC) time zone. Times up to and including 23:59:59 December 31, 2049 UTC shall be encoded as UTCTime as

YYMMDDHHmmssZ.

Times later than 23:59:59 December 31, 2049 UTC shall be encoded as GeneralizedTime as

YYYYMMDDHHmmssZ.

Not Before Date

The earliest time a Certificate may be used (notBefore). This shall be the time the Certificate is created.

Not After Date

The latest time a Certificate is expected to be used (`notAfter`). Certificates are expected to operate indefinitely into the future and should use the value 99991231235959Z. Systems and Secure SMETS1 Devices verifying a Certificate are expected to accept this value indefinitely.

Subject X520 Common Name

This field shall be populated with the following values:

```
C = GB
S = Hampshire
L = Winchester
OU = Secure Meters (UK) Ltd
O = Secure Meters (UK) Ltd
CN = SML-MFG Operations CA
```

Key Usage

The `keyUsage` extension should be populated as follows:

`keyCertSign;` and

`cRLSign`

Basic Constraints

The `BasicConstraints` extension should be populated as follows:

```
cA=TRUE
pathLen=Absent
```

Subject Public Key Info

The Certificate's `subjectPublicKeyInfo` field shall indicate the Public Key algorithm identifier and the Public Key in the specified algorithm format as specified in RFC 3279 and RFC 5480.

The algorithm field in the `subjectPublicKeyInfo` structure shall contain the following identifier:

```
        id-ecPublicKey OBJECT IDENTIFIER ::= {iso(1) member-body(2)
        us(840) ansi-X9-62(10045) keyType(2) 1 }
```

`id-ecPublicKey` indicates that the algorithms that can be used with the subject Public Key are unrestricted. The key is only restricted by the values indicated in the key usage Certificate extension (explained further under the next **extensions** heading).

The parameter for `id-ecPublicKey` is as follows and shall always be present:

```
    ECParameters ::= CHOICE {

namedCurve          OBJECT IDENTIFIER         -

- implicitCurve   NULL         --

specifiedCurve  SpecifiedECDomain

      }
```

Only the following field in ECParameters shall be used: o

`namedCurve` - identifies all the required values for a particular set

of elliptic curve domain parameters to be represented by an

`OBJECT IDENTIFIER`.

The object identifier for the curve choice to be used in Certificates is:

```
secp256r1 OBJECT IDENTIFIER ::= { iso(1) member-body(2) us(840)
ansi-X9-62(10045) curves(3) prime(1) 7 }
```

The `subjectPublicKey` from `SubjectPublicKeyInfo` is the ECC Public Key.

Implementations of Elliptic Curve Cryptography according to this document shall only support the uncompressed form.

The first octet of the `subjectPublicKey` indicates whether the key is compressed or uncompressed. The uncompressed form is indicated by 0x04 (the compressed form is indicated by either 0x02 or 0x03). The Public Key MUST be rejected if any value other than 0x04 is included in the first octet.

Signature Algorithm

The `signatureAlgorithm` field shall indicate the Root SS1SPCA signature algorithm used to sign this Certificate as defined under the next **Signature Method (ECDSA)** heading.

Signature Value

The Root SS1SPCA's signature of the Certificate shall be computed using the Root SS1SPCA's private signing key using the algorithm identified under the next **Signature Method (ECDSA)** heading.

The structure for ECDSA signatures shall be as per RFC 5480.

Cryptographic Primitives for Signature Method

Signature Method (ECDSA)

The ECDSA signature method is defined in NIST FIPS 186-4. When implementing ECDSA, the SHA-256 message digest algorithm and the P-256 elliptic curve as defined in FIPS 186-4 Annex D, D.1.2.3, shall be used.

The signature algorithm shall be `ecdsa-with-SHA256` as specified in RFC 5759 and 6318. The algorithm identifier is:

```
ecdsa-with-SHA256 OBJECT IDENTIFIER ::= { iso(1) memberbody(2)
us(840) ansi-X9-62(10045) signatures(4) ecdsa-withsha2(3) 2 }
```

SHA-256 hash algorithm

The hash algorithm used shall be the SHA-256 secure hash algorithm as defined in NIST FIPS 180-4.

11.12 Subordinate SS1SPCA Certificate Profile - SMSO CA

Field Name	RFC 5759/5280 Type	Value	Reference
version	INTEGER	v3	
serialNumber	INTEGER	Positive Integer	
signature	AlgorithmIdentifi er	SHA256 with ECDSA	
The value field of the AttributeTypeAndV alue structure within the subject field whose type is id-at-commonName (the "Issuer X520 Common Name")	UTF8String	Globally unique name of Intermediate SS1SPCA (as defined in the Intermediate SS1SPCA Certificate Profile)	
keyIdentifier in subjectKeyIdentif ier (the "Subject Key Identifier")	keyIdentifier	Provides a means for identifying certificates containing the particular Public Key used in an application	
keyIdentifier in authorityKeyIdent ifier (the "Authority Key Identifier")	keyIdentifier	A unique value that matches the subjectKeyIdent ifier value of the issuer's credential	
notBefore	Time	Creation time of the certificate	

notAfter	Time	shall be assigned the GeneralizedTime value of 99991231235959Z	
The value field of the AttributeTypeAndValue structure within the subject field whose type is id-atcommonName (the "Subject X520 Common Name")	UTF8String	Globally unique name of Subordinate SS1SPCA	
Key Usage	keyUsage	The permitted Key Usages.	
Basic Constraints	BasicConstraints	The permitted Basic Constraints values.	
subjectPublicKeyI nfo	SubjectPublicKeyI nfo	The Subject's Public Key	
signatureAlgorithm	AlgorithmIdentifier	SHA256 with ECDSA	
signatureValue	BIT STRING	Subject certificate signature	

Version

The version of the X.509 Certificate. Valid Certificates shall identify themselves as version 3.

Serial Number

Certificate serial number which is a positive integer. The `serialNumber` identifies the Certificate and shall be created by the SS1SPCA that signs the Certificate. The `serialNumber` shall be unique in the scope of Certificates signed by the Intermediate SS1SPCA.

Signature

The identity of the signature algorithm used to sign the Certificate. The field is identical to the value of the Intermediate SS1SPCA Certificate's `signatureAlgorithm` field explained further under the next **signatureAlgorithm** heading.

Issuer X520 Common Name

The name of the signer of the Certificate. This will be the globally unique name of the Intermediate SS1SPCA (as defined in the Intermediate SS1SPCACertificate Profile).

Subject Key Identifier

The `subjectKeyIdentifier` extension should be included and marked as non-critical in the Certificate.

Authority Key Identifier

To optimize building the correct credential chain, the non-critical `authorityKeyIdentifier` extension shall be populated with a unique value as recommended by RFC 5280 and shall be included in all SS1SP End Entity Certificates.

Validity

The time period over which the issuer expects the Certificate to be valid. The validity period is the period of time from notBefore through notAfter, inclusive.

Subordinate SS1SPCA Certificates are expected to operate indefinitely into the future and should use the value 99991231235959Z. Solutions verifying a Subordinate SS1SPCA Certificate are expected to accept this value indefinitely.

All times shall be stated in the Universal Coordinated Time (UTC) time zone. Times up to and including 23:59:59 December 31, 2049 UTC shall be encoded as UTCTime as YYMMDDHHmmssZ.

Times later than 23:59:59 December 31, 2049 UTC shall be encoded as GeneralizedTime as YYYYMMDDHHmmssZ.

Not Before Date

The earliest time a Certificate may be used (notBefore). This shall be the time the Certificate is created.

Not After Date

The latest time a Certificate is expected to be used (notAfter). Certificates are expected to operate indefinitely into the future and should use the value 99991231235959Z. Systems and Secure SMETS1 Devices verifying a Certificate are expected to accept this value indefinitely.

Subject X520 Common Name

This field shall be populated with the following values:

```
C = GB
```

```
S = Hampshire
L = Winchester
OU = Secure Meters (UK) Ltd
O = Secure Meters (UK) Ltd
CN = SML-HES CA
```

Key Usage

The `keyUsage` extension should be populated as follows:

`keyCertSign;` and

`cRLSign`

Basic Constraints

The `BasicConstraints` extension should be populated as follows:

```
cA=TRUE
pathLen=Absent
```

Subject Public Key Info

The Certificate's `subjectPublicKeyInfo` field shall indicate the Public Key algorithm identifier and the Public Key in the specified algorithm format as specified in RFC 3279 and RFC 5480.

The algorithm field in the `subjectPublicKeyInfo` structure shall contain the following identifier:

```
        id-ecPublicKey OBJECT IDENTIFIER ::= {iso(1) member-body(2)
        us(840) ansi-X9-62(10045) keyType(2) 1 }
```

id-ecPublicKey indicates that the algorithms that can be used with the subject Public Key are unrestricted. The key is only restricted by the values indicated in the key usage Certificate extension (explained further under the next **extensions** heading).

The parameter for id-ecPublicKey is as follows and shall always be present:

```
    ECParameters ::= CHOICE {
namedCurve          OBJECT IDENTIFIER         -
- implicitCurve    NULL         --
specifiedCurve  SpecifiedECDomain
      }
```

Only the following field in ECParameters shall be used: o

namedCurve - identifies all the required values for a particular set

of elliptic curve domain parameters to be represented by an

OBJECT IDENTIFIER.

The object identifier for the curve choice to be used in Certificates is:

```
        secp256r1 OBJECT IDENTIFIER ::= { iso(1) member-body(2) us(840)
        ansi-X9-62(10045) curves(3) prime(1) 7 }
```

The subjectPublicKey from SubjectPublicKeyInfo is the ECC Public Key.

Implementations of Elliptic Curve Cryptography according to this document shall only support the uncompressed form.

The first octet of the `subjectPublicKey` indicates whether the key is compressed or uncompressed. The uncompressed form is indicated by 0x04 (the compressed form is indicated by either 0x02 or 0x03). The Public Key MUST be rejected if any value other than 0x04 is included in the first octet.

Signature Algorithm

The `signatureAlgorithm` field shall indicate the Intermediate SS1SPCA signature algorithm used to sign this Certificate as defined under the next **Signature Method (ECDSA)** heading.

Signature Value

The Intermediate SS1SPCA's signature of the Certificate shall be computed using the Intermediate SS1SPCA's private signing key using the algorithm identified under the next **Signature Method (ECDSA)** heading.

The structure for ECDSA signatures shall be as per RFC 5480.

Cryptographic Primitives for Signature Method

Signature Method (ECDSA)

The ECDSA signature method is defined in NIST FIPS 186-4. When implementing ECDSA, the SHA-256 message digest algorithm and the P-256 elliptic curve as defined in FIPS 186-4 Annex D, D.1.2.3, shall be used.

The signature algorithm shall be `ecdsa-with-SHA256` as specified in RFC 5759 and 6318. The algorithm identifier is:

```
ecdsa-with-SHA256 OBJECT IDENTIFIER ::= { iso(1) memberbody(2)
us(840) ansi-X9-62(10045) signatures(4) ecdsa-withsha2(3) 2 }
```

SHA-256 hash algorithm

The hash algorithm used shall be the SHA-256 secure hash algorithm as defined in NIST FIPS 180-4.

11.13 Subordinate SS1SPCA Certificate Profile - SMSO KMS CA

Field Name	RFC 5759/5280 Type	Value	Reference
version	INTEGER	v3	
serialNumber	INTEGER	Positive Integer	
signature	AlgorithmIdentifier	SHA256 with ECDSA	
The value field of the AttributeTypeAndValue structure within the subject field whose type is id-at-commonName (the "Issuer X520 Common Name")	UTF8String	Globally unique name of Intermediate SS1SPCA (as defined in the Intermediate SS1SPCA Certificate Profile)	
keyIdentifier in subjectKeyIdentif ier (the "Subject Key Identifier")	keyIdentifier	Provides a means for identifying certificates containing the particular Public Key used in an application	
keyIdentifier in authorityKeyIdentifier (the "Authority Key Identifier")	keyIdentifier	A unique value that matches the subjectKeyIdentifier value of the issuer's credential	

notBefore	Time	Creation time of the certificate	
notAfter	Time	shall be assigned the GeneralizedTime value of 99991231235959Z	
The value field of the AttributeTypeAndValue structure within the subject field whose type is id-atcommonName (the “Subject X520 Common Name”)	UTF8String	Globally unique name of Subordinate SS1SPCA	
Key Usage	keyUsage	The permitted Key Usages.	
Basic Constraints	BasicConstraints	The permitted Basic Constraints values.	
subjectPublicKeyI nfo	SubjectPublicKeyI nfo	The Subject’s Public Key	
signatureAlgorithm	AlgorithmIdentifier	SHA256 with ECDSA	
signatureValue	BIT STRING	Subject certificate signature	

Version

The version of the X.509 Certificate. Valid Certificates shall identify themselves as version 3.

Serial Number

Certificate serial number which is a positive integer. The `serialNumber` identifies the Certificate and shall be created by the SS1SPCA that signs the Certificate. The `serialNumber` shall be unique in the scope of Certificates signed by the Intermediate SS1SPCA.

Signature

The identity of the signature algorithm used to sign the Certificate. The field is identical to the value of the Intermediate SS1SPCA Certificate's `signatureAlgorithm` field explained further under the next **signatureAlgorithm** heading.

Issuer X520 Common Name

The name of the signer of the Certificate. This will be the globally unique name of the Intermediate SS1SPCA (as defined in the Intermediate SS1SPCACertificate Profile).

Subject Key Identifier

The `subjectKeyIdentifier` extension should be included and marked as non-critical in the Certificate.

Authority Key Identifier

To optimize building the correct credential chain, the non-critical authorityKeyIdentifier extension shall be populated with a unique value as recommended by RFC 5280 and shall be included in all SS1SP End Entity Certificates.

Validity

The time period over which the issuer expects the Certificate to be valid. The validity period is the period of time from notBefore through notAfter, inclusive.

Subordinate SS1SPCA Certificates are expected to operate indefinitely into the future and should use the value 99991231235959Z. Solutions verifying a Subordinate SS1SPCA Certificate are expected to accept this value indefinitely.

All times shall be stated in the Universal Coordinated Time (UTC) time zone. Times up to and including 23:59:59 December 31, 2049 UTC shall be encoded as UTCTime as YYMMDDHHmmssZ.

Times later than 23:59:59 December 31, 2049 UTC shall be encoded as GeneralizedTime as YYYYMMDDHHmmssZ.

Not Before Date

The earliest time a Certificate may be used (notBefore). This shall be the time the Certificate is created.

Not After Date

The latest time a Certificate is expected to be used (`notAfter`). Certificates are expected to operate indefinitely into the future and should use the value 99991231235959Z. Systems and Secure SMETS1 Devices verifying a Certificate are expected to accept this value indefinitely.

Subject X520 Common Name

This field shall be populated with the following values:

```
C = GB

S = Hampshire

L = Winchester

OU = Secure Meters (UK) Ltd

O = Secure Meters (UK) Ltd

CN = SML-Key Management CA
```

Key Usage

The `keyUsage` extension should be populated as follows:

`keyCertSign;` and

`cRLSign`

Basic Constraints

The `BasicConstraints` extension should be populated as follows:

```
cA=TRUE

pathLen=Absent
```

Subject Public Key Info

The Certificate's `subjectPublicKeyInfo` field shall indicate the Public Key algorithm identifier and the Public Key in the specified algorithm format as specified in RFC 3279 and RFC 5480.

The algorithm field in the `subjectPublicKeyInfo` structure shall contain the following identifier:

```
        id-ecPublicKey OBJECT IDENTIFIER ::= {iso(1) member-body(2)
        us(840) ansi-X9-62(10045) keyType(2) 1 }
```

`id-ecPublicKey` indicates that the algorithms that can be used with the subject Public Key are unrestricted. The key is only restricted by the values indicated in the key usage Certificate extension (explained further under the next **extensions** heading).

The parameter for `id-ecPublicKey` is as follows and shall always be present:

```
    ECParameters ::= CHOICE {
namedCurve          OBJECT IDENTIFIER         -
- implicitCurve   NULL         --
specifiedCurve  SpecifiedECDomain
      }
```

Only the following field in ECParameters shall be used: o

`namedCurve` - identifies all the required values for a particular set

of elliptic curve domain parameters to be represented by an

`OBJECT IDENTIFIER`.

The object identifier for the curve choice to be used in Certificates is:

```
secp256r1 OBJECT IDENTIFIER ::= { iso(1) member-body(2) us(840)
ansi-X9-62(10045) curves(3) prime(1) 7 }
```

The subjectPublicKey from SubjectPublicKeyInfo is the ECC Public Key.

Implementations of Elliptic Curve Cryptography according to this document shall only support the uncompressed form.

The first octet of the subjectPublicKey indicates whether the key is compressed or uncompressed. The uncompressed form is indicated by 0x04 (the compressed form is indicated by either 0x02 or 0x03). The Public Key MUST be rejected if any value other than 0x04 is included in the first octet.

Signature Algorithm

The signatureAlgorithm field shall indicate the Intermediate SS1SPCA signature algorithm used to sign this Certificate as defined under the next **Signature Method (ECDSA)** heading.

Signature Value

The Intermediate SS1SPCA's signature of the Certificate shall be computed using the Intermediate SS1SPCA's private signing key using the algorithm identified under the next **Signature Method (ECDSA)** heading.

The structure for ECDSA signatures shall be as per RFC 5480.

Cryptographic Primitives for Signature Method

Signature Method (ECDSA)

The ECDSA signature method is defined in NIST FIPS 186-4. When implementing ECDSA, the SHA-256 message digest algorithm and the P-256 elliptic curve as defined in FIPS 186-4 Annex D, D.1.2.3, shall be used.

The signature algorithm shall be `ecdsa-with-SHA256` as specified in RFC 5759 and 6318.

The algorithm identifier is:

```
ecdsa-with-SHA256 OBJECT IDENTIFIER ::= { iso(1) memberbody(2)
us(840) ansi-X9-62(10045) signatures(4) ecdsa-withsha2(3) 2 }
```

SHA-256 hash algorithm

The hash algorithm used shall be the SHA-256 secure hash algorithm as defined in NIST FIPS 180-4.

11.14 Subordinate SS1SPCA Certificate Profile - SMSO Code Signing CA

Field Name	RFC 5759/5280 Type	Value	Reference
version	INTEGER	v3	
serialNumber	INTEGER	Positive Integer	
signature	AlgorithmIdentifier	SHA256 with ECDSA	
The value field of the AttributeTypeAndValue structure within the subject field whose type is id-at-commonName (the "Issuer X520 Common Name")	UTF8String	Globally unique name of Intermediate SS1SPCA (as defined in the Intermediate SS1SPCA Certificate Profile)	
keyIdentifier in subjectKeyIdentif ier (the "Subject Key Identifier")	keyIdentifier	Provides a means for identifying certificates containing the particular Public Key used in an application	
keyIdentifier in authorityKeyIdentifier (the "Authority Key Identifier")	keyIdentifier	A unique value that matches the subjectKeyIdentifier value of the issuer's credential	

`notBefore`	`Time`	Creation time of the certificate	
`notAfter`	`Time`	shall be assigned the `GeneralizedTime` value of 99991231235959Z	
The `value` field of the `AttributeTypeAndValue` structure within the `subject` field whose `type` is `id-atcommonName` (the “Subject X520 Common Name”)	`UTF8String`	Globally unique name of Subordinate SS1SPCA	
Key Usage	`keyUsage`	The permitted Key Usages.	
Basic Constraints	`BasicConstraints`	The permitted Basic Constraints values.	
`subjectPublicKeyI nfo`	`SubjectPublicKeyI nfo`	The Subject’s Public Key	
`signatureAlgorithm`	`AlgorithmIdentifier`	SHA256 with ECDSA	
`signatureValue`	`BIT STRING`	Subject certificate signature	

Version

The version of the X.509 Certificate. Valid Certificates shall identify themselves as version 3.

Serial Number

Certificate serial number which is a positive integer. The `serialNumber` identifies the Certificate and shall be created by the SS1SPCA that signs the Certificate. The `serialNumber` shall be unique in the scope of Certificates signed by the Intermediate SS1SPCA.

Signature

The identity of the signature algorithm used to sign the Certificate. The field is identical to the value of the Intermediate SS1SPCA Certificate's `signatureAlgorithm` field explained further under the next **signatureAlgorithm** heading.

Issuer X520 Common Name

The name of the signer of the Certificate. This will be the globally unique name of the Intermediate SS1SPCA (as defined in the Intermediate SS1SPCACertificate Profile).

Subject Key Identifier

The `subjectKeyIdentifier` extension should be included and marked as non-critical in the Certificate.

Authority Key Identifier

To optimize building the correct credential chain, the non-critical `authorityKeyIdentifier` extension shall be populated with a unique value as recommended by RFC 5280 and shall be included in all SS1SP End Entity Certificates.

Validity

The time period over which the issuer expects the Certificate to be valid. The `validity` period is the period of time from `notBefore` through `notAfter`, inclusive.

Subordinate SS1SPCA Certificates are expected to operate indefinitely into the future and should use the value 99991231235959Z. Solutions verifying a Subordinate SS1SPCA Certificate are expected to accept this value indefinitely.

All times shall be stated in the Universal Coordinated Time (UTC) time zone. Times up to and including 23:59:59 December 31, 2049 UTC shall be encoded as `UTCTime` as YYMMDDHHmmssZ.

Times later than 23:59:59 December 31, 2049 UTC shall be encoded as `GeneralizedTime` as YYYYMMDDHHmmssZ.

Not Before Date

The earliest time a Certificate may be used (`notBefore`). This shall be the time the Certificate is created.

Not After Date

The latest time a Certificate is expected to be used (`notAfter`). Certificates are expected to operate indefinitely into the future and should use the value 99991231235959Z. Systems and Secure SMETS1 Devices verifying a Certificate are expected to accept this value indefinitely.

Subject X520 Common Name

This field shall be populated with the following values:

```
C = GB

S = Hampshire

L = Winchester

OU = Secure Meters (UK) Ltd

O = Secure Meters (UK) Ltd

CN = SML-Code Signing CA
```

Key Usage

The `keyUsage` extension should be populated as follows:

`keyCertSign;` and
`cRLSign`

Basic Constraints

The `BasicConstraints` extension should be populated as follows:

```
cA=TRUE

pathLen=Absent
```

Subject Public Key Info

The Certificate's `subjectPublicKeyInfo` field shall indicate the Public Key algorithm identifier and the Public Key in the specified algorithm format as specified in RFC 3279 and RFC 5480.

The algorithm field in the `subjectPublicKeyInfo` structure shall contain the following identifier:

```
        id-ecPublicKey OBJECT IDENTIFIER ::= {iso(1) member-body(2)
        us(840) ansi-X9-62(10045) keyType(2) 1 }
```

`id-ecPublicKey` indicates that the algorithms that can be used with the subject Public Key are unrestricted. The key is only restricted by the values indicated in the key usage Certificate extension (explained further under the next **extensions** heading).

The parameter for `id-ecPublicKey` is as follows and shall always be present:

```
    ECParameters ::= CHOICE {
namedCurve         OBJECT IDENTIFIER        -
- implicitCurve   NULL        --
specifiedCurve  SpecifiedECDomain
     }
```

Only the following field in ECParameters shall be used: o

`namedCurve` - identifies all the required values for a particular set of elliptic curve domain parameters to be represented by an `OBJECT IDENTIFIER`.

The object identifier for the curve choice to be used in Certificates is:

```
secp256r1 OBJECT IDENTIFIER ::= { iso(1) member-body(2) us(840)
ansi-X9-62(10045) curves(3) prime(1) 7 }
```

The `subjectPublicKey` from `SubjectPublicKeyInfo` is the ECC Public Key.

Implementations of Elliptic Curve Cryptography according to this document shall only support the uncompressed form.

The first octet of the `subjectPublicKey` indicates whether the key is compressed or uncompressed. The uncompressed form is indicated by 0x04 (the compressed form is indicated by either 0x02 or 0x03). The Public Key MUST be rejected if any value other than 0x04 is included in the first octet.

Signature Algorithm

The `signatureAlgorithm` field shall indicate the Intermediate SS1SPCA signature algorithm used to sign this Certificate as defined under the next **Signature Method (ECDSA)** heading.

Signature Value

The Intermediate SS1SPCA's signature of the Certificate shall be computed using the Intermediate SS1SPCA's private signing key using the algorithm identified under the next **Signature Method (ECDSA)** heading.

The structure for ECDSA signatures shall be as per RFC 5480.

Cryptographic Primitives for Signature Method

Signature Method (ECDSA)

The ECDSA signature method is defined in NIST FIPS 186-4. When implementing ECDSA, the SHA-256 message digest algorithm and the P-256 elliptic curve as defined in FIPS 186-4 Annex D, D.1.2.3, shall be used.

The signature algorithm shall be `ecdsa-with-SHA256` as specified in RFC 5759 and 6318.

The algorithm identifier is:

```
ecdsa-with-SHA256 OBJECT IDENTIFIER ::= { iso(1) memberbody(2)
us(840) ansi-X9-62(10045) signatures(4) ecdsa-withsha2(3) 2 }
```

SHA-256 hash algorithm

The hash algorithm used shall be the SHA-256 secure hash algorithm as defined in NIST FIPS 180-4.

11.15 Subordinate SS1SPCA Certificate Profile - Device CA

Field Name	RFC 5759/5280 Type	Value	Reference
version	INTEGER	v3	
serialNumber	INTEGER	Positive Integer	
signature	AlgorithmIdentifier	SHA256 with ECDSA	
The value field of the AttributeTypeAndValue structure within the subject field whose type is id-at-commonName (the "Issuer X520 Common Name")	UTF8String	Globally unique name of Intermediate SS1SPCA (as defined in the Intermediate SS1SPCA Certificate Profile)	
keyIdentifier in subjectKeyIdentif ier (the "Subject Key Identifier")	keyIdentifier	Provides a means for identifying certificates containing the particular Public Key used in an application	
keyIdentifier in authorityKeyIdentifier (the "Authority Key Identifier")	keyIdentifier	A unique value that matches the subjectKeyIdentifier value of the issuer's credential	

notBefore	Time	Creation time of the certificate	
notAfter	Time	shall be assigned the GeneralizedTime value of 99991231235959Z	
The value field of the AttributeTypeAndValue structure within the subject field whose type is id-atcommonName (the “Subject X520 Common Name”)	UTF8String	Globally unique name of Subordinate SS1SPCA	
Key Usage	keyUsage	The permitted Key Usages.	
Basic Constraints	BasicConstraints	The permitted Basic Constraints values.	
subjectPublicKeyI nfo	SubjectPublicKeyI nfo	The Subject’s Public Key	
signatureAlgorithm	AlgorithmIdentifier	SHA256 with ECDSA	
signatureValue	BIT STRING	Subject certificate signature	

Version

The version of the X.509 Certificate. Valid Certificates shall identify themselves as version 3.

Serial Number

Certificate serial number which is a positive integer. The `serialNumber` identifies the Certificate and shall be created by the SS1SPCA that signs the Certificate. The `serialNumber` shall be unique in the scope of Certificates signed by the Intermediate SS1SPCA.

Signature

The identity of the signature algorithm used to sign the Certificate. The field is identical to the value of the Intermediate SS1SPCA Certificate's `signatureAlgorithm` field explained further under the next **signatureAlgorithm** heading.

Issuer X520 Common Name

The name of the signer of the Certificate. This will be the globally unique name of the Intermediate SS1SPCA (as defined in the Intermediate SS1SPCACertificate Profile).

Subject Key Identifier

The `subjectKeyIdentifier` extension should be included and marked as non-critical in the Certificate.

Authority Key Identifier

To optimize building the correct credential chain, the non-critical `authorityKeyIdentifier` extension shall be populated with a unique value as recommended by RFC 5280 and shall be included in all SS1SP End Entity Certificates.

Validity

The time period over which the issuer expects the Certificate to be valid. The `validity` period is the period of time from `notBefore` through `notAfter`, inclusive.

Subordinate SS1SPCA Certificates are expected to operate indefinitely into the future and should use the value 99991231235959Z. Solutions verifying a Subordinate SS1SPCA Certificate are expected to accept this value indefinitely.

All times shall be stated in the Universal Coordinated Time (UTC) time zone. Times up to and including 23:59:59 December 31, 2049 UTC shall be encoded as `UTCTime` as YYMMDDHHmmssZ.

Times later than 23:59:59 December 31, 2049 UTC shall be encoded as `GeneralizedTime` as YYYYMMDDHHmmssZ.

Not Before Date

The earliest time a Certificate may be used (`notBefore`). This shall be the time the Certificate is created.

Not After Date

The latest time a Certificate is expected to be used (`notAfter`). Certificates are expected to operate indefinitely into the future and should use the value 99991231235959Z. Systems and Secure SMETS1 Devices verifying a Certificate are expected to accept this value indefinitely.

Subject X520 Common Name

This field shall be populated with the following values:

C = IN

S = Rajasthan

L = Udaipur

OU = Secure Meters Ltd

O = Secure Meters Ltd

CN = Secure Meters Production CA

Key Usage

The keyUsage extension should be populated as follows:

keyCertSign; and

cRLSign

Basic Constraints

The BasicConstraints extension should be populated as follows:

cA=TRUE

pathLen=Absent

Subject Public Key Info

The Certificate's subjectPublicKeyInfo field shall indicate the Public Key algorithm identifier and the Public Key in the specified algorithm format as specified in RFC 3279 and RFC 5480.

The algorithm field in the subjectPublicKeyInfo structure shall contain the following identifier:

```
        id-ecPublicKey OBJECT IDENTIFIER ::= {iso(1) member-body(2)
        us(840) ansi-X9-62(10045) keyType(2) 1 }
```

`id-ecPublicKey` indicates that the algorithms that can be used with the subject Public Key are unrestricted. The key is only restricted by the values indicated in the key usage Certificate extension (explained further under the next **extensions** heading).

The parameter for `id-ecPublicKey` is as follows and shall always be present:

```
    ECParameters ::= CHOICE {
namedCurve          OBJECT IDENTIFIER         -
- implicitCurve   NULL        --
specifiedCurve  SpecifiedECDomain
     }
```

Only the following field in ECParameters shall be used: o

`namedCurve` - identifies all the required values for a particular   set

of elliptic curve domain parameters to be represented by an

`OBJECT IDENTIFIER`.

The object identifier for the curve choice to be used in Certificates is:

```
        secp256r1 OBJECT IDENTIFIER ::= { iso(1) member-body(2) us(840)
        ansi-X9-62(10045) curves(3) prime(1) 7 }
```

The `subjectPublicKey` from `SubjectPublicKeyInfo` is the ECC Public Key.

Implementations of Elliptic Curve Cryptography according to this document shall only support the uncompressed form.

The first octet of the subjectPublicKey indicates whether the key is compressed or uncompressed. The uncompressed form is indicated by 0x04 (the compressed form is indicated by either 0x02 or 0x03). The Public Key MUST be rejected if any value other than 0x04 is included in the first octet.

Signature Algorithm

The signatureAlgorithm field shall indicate the Intermediate SS1SPCA signature algorithm used to sign this Certificate as defined under the next **Signature Method (ECDSA)** heading.

Signature Value

The Intermediate SS1SPCA's signature of the Certificate shall be computed using the Intermediate SS1SPCA's private signing key using the algorithm identified under the next **Signature Method (ECDSA)** heading.

The structure for ECDSA signatures shall be as per RFC 5480.

Cryptographic Primitives for Signature Method

Signature Method (ECDSA)

The ECDSA signature method is defined in NIST FIPS 186-4. When implementing ECDSA, the SHA-256 message digest algorithm and the P-256 elliptic curve as defined in FIPS 186-4 Annex D, D.1.2.3, shall be used.

The signature algorithm shall be ecdsa-with-SHA256 as specified in RFC 5759 and 6318. The algorithm identifier is:

```
ecdsa-with-SHA256 OBJECT IDENTIFIER ::= { iso(1) memberbody(2)
us(840) ansi-X9-62(10045) signatures(4) ecdsa-withsha2(3) 2 }
```

SHA-256 hash algorithm

The hash algorithm used shall be the SHA-256 secure hash algorithm as defined in NIST FIPS 180-4.

12 Annex C: Subscriber Obligations

12.1 Certificate Signing Requests

(A) Each Eligible Subscriber shall ensure that all of the information contained in each Certificate Signing Request made by it conform with the relevant Certificate Profiles as set out in Annex B of this Policy.

(B) No Eligible Subscriber may make a Certificate Signing Request which contains:

(i) any information that constitutes a trade mark, unless it is the holder of the Intellectual Property Rights in relation to that trade mark; or

(ii) any confidential information which would be contained in a Certificate Issued in response to that Certificate Signing Request.

(A) Each Eligible Subscriber shall ensure that the Public Key that is included within a Certificate Signing Request is part of a Key Pair that has been generated using random numbers which are such as to make it computationally infeasible to regenerate that Key Pair even with knowledge of when and by means of what equipment it was generated.

(B) An Eligible Subscriber shall take all reasonable steps to ensure that a Certificate Signing Request for the Issue of a Certificate does not contain the same Public Key as a Public Key which that Eligible Subscriber knows to be contained in any other Certificate.

12.2 Subscribing for or Rejecting Certificates

(A) Where any Certificate is Issued to an Eligible Subscriber in response to a Certificate Signing Request, that Eligible Subscriber shall:

(i) establish whether the information contained in that Certificate is consistent with information that was contained in the Certificate Signing Request;

(ii) if it identifies that the Certificate contains any information which is untrue or inaccurate:

(a) reject that Certificate; and

(b) inform the SS1SPA that it rejects the Certificate; and

(iii) where it does not reject the Certificate, become a Subscriber for that Certificate.

12.3 Use of Certificates and Key Pairs

(A) Each Subscriber shall ensure that it does not use any Certificate, Public Key contained within a Certificate, or Private Key associated with a Public Key contained in a Certificate, that is held by it other than for the purposes set out in Part 1.4.1 of this Policy.

12.4 SS1SPCA Certificates: Expiry of Validity Period

(i) Each Subscriber for a Certificate as set out in Part 3.3.1 (b) of this Policy shall, prior to the expiry of the Validity Period that Certificate for which it is the Subscriber, request a re-key for that Certificate by applying for the Issue of a new Certificate in accordance with the provisions of this Policy.

13 Annex D: Relying Party Obligations

13.1 Relying Parties

(A) For the purposes of this Section Annex D, a ‘Relying Party’ in relation to a Certificate means the Secure S1SP which relies on the Certificate for the purposes as set out in Part 1.4 of this Policy in order to meet its security obligations to its customers as set out in their respective contractual arrangements.

13.2 Duties in relation to Certificates

(A) The Relying Party shall not rely on a Certificate where the Validity Period of that Certificate has expired.

(B) The Relying Party shall not rely on a Certificate where it suspects that the Certificate has been Compromised.

(C) The Relying Party shall take reasonable steps, by means of appropriate Systems, to verify Digital Signatures, Check Cryptographic Protection, Confirm Validity and perform other appropriate cryptographic operations before relying on any Certificate.

14 Annex E: SS1SP PKI RAPP

14.1 Purpose

(A) This Annex E: SS1SP PKI RAPP sets out the high level principle obligations and activities undertaken by the SS1SPCA in its capacity as the SS1SP PKI Registration Authority in accordance with this Policy. The SS1SP RAPP also sets out the activities undertaken by the SS1SP PKI Registration Authority in support of the procedures as set out in this Section.

14.2 SS1SP PKI RAPP Principles

(A) All Certificates requested and Certificates issued under the auspices of the SS1SPCA must be:

(i) compliant with PKCS#10;

(ii) DER encoded

(iii) compliant with the Certificate Profiles as set out in Annex B of this Policy

(iv) compliant with the obligations as set out in Annex C of this Policy.

14.3 SS1SP PKI Registration Authority Roles

(A) The SS1SP PKI RA consists of the following roles:

(i) SS1SPCA Systems technical RA role; and

(ii) SS1SPCA Personnel requesting and approving Certificates for issuance.

(B) The Subordinate SS1SPCA Device CA acts as a technical RA for Certificates requested by Secure SMETS1 Devices only. The SS1SPCA Systems have been authorised to act as technical RAs through a combination of access controls and IP whitelisting. Only valid Secure SMETS1 Devices may request a Certificate. Therefore, acting as an Authorised Subscriber for such SS1SP End Entity Certificates.

(C) Authorised and approved SS1SPCA Personnel are responsible for requesting and issuing all other SS1SPCA End Entity Certificates using SS1SPA Systems. Thereby acting as an Authorised Subscriber.

(D) Only SS1SPCA Personnel with Privileged User rights can request and approve Certificate requests through the SS1SPCA Systems. This is enforced through:

(i) Pre-authorised and pre-approved access to SS1SPCA Systems for such SS1SPCA Personnel;

(ii) Access control to the SS1SPCA Systems;

(iii) User account management (audit and logging);

(iv) Dedicated named accounts on the SS1SPCA System;

(E) Prior to being granted access to SS1SPCA Systems, all such SS1SPCA Personnel with Privileged User rights will either have:

(i) identities checked in line with personnel security standard BS7858;

(ii) background clearance checks performed in accordance with security check (SC) cleared to an appropriate level (in accordance with the latest version of the HMG Cabinet Office Security Policy; and/or

(iii) Screening and background verifications equivalent to BS7858. The personnel and key personnel, based in India, engaged in providing support for Smart metering services and solutions shall comply at all times with a background verification equivalent to personnel security British Standard BS 7858:2012 (Security Screening of Individuals Employed in Security Environment - Code of Practice),

14.4 Eligible and authorised subscribers

(A) Only those systems and SS1SPCA Personnel described in Part 14.3 of this Policy are Authorised to Subscribe for Certificates under the auspices of the SS1SP PKI. At the point of the SS1SP PKI RA approving such systems or SS1SPCA Personnel they become Authorised Subscribers.

(B) An Authorised Subscriber is an Eligible Subscriber in respect to the following:

(i) SS1SPCA Personnel who are Authorised Subscribers are Eligible Subscribers for the following SS1SPCA End Entity Certificates only:

(a) SMSO TLS Certificate;

(b) SMSO KMS Certificate; and

(c) Code Signing Certificate.

(ii) SS1SPA Systems who are Authorised Subscribers are Eligible Subscribers for the following SS1SPCA End Entity Certificate only:

(a) Device Certificate,

14.5 SS1SP PKI Technical RA Verification and Issuance of Certificate

(A) The Subordinate SS1SPCA Device CA performs the following technical RA check in response to a Certificate Signing Request from a Secure SMETS1 Device:

(i) The SS1SPCA Root Certificate is loaded on the Secure SMETS1 Device at point of manufacture;

(ii) The Secure SMETS1 Device generates a Certificate Signing Request using a Private Key generated on the Secure SMETS1 Device within the manufacturing facility;

(iii) The Certificate Signing Request is sent to a production central system (which incorporates the SS1SPCA Device CA) in PKCS#10 file format.

(iv) The production central system verifies the Certificate Signing Request against the production record it holds for each Secure SMETS1 Device (Device serial number and Device model) as well as performing a proof of possession check using the PKCS#10 format.

(v) If the production central system finds a match between its records and the Secure SMETS1 Device serial number and Secure SMETS1 Device model within the CSR, and it is expecting to manufacture such Secure SMETS1 Device, then:

(a) it passes the CSR to the Device CA to process the Certificate Signing Request;

(b) The Device CA then:

(1) signs the SS1SP End Entity Certificate for the Secure SMETS1 Device; and

(2) sends the SS1SP End Entity Certificate along with the SS1SPCA Certificate chain (in PKCS#7 file format) to the Secure SMETS1 Device.

(c) The Secure SMETS1 Device then verifies the SS1SP End Entity Certificate as well as performing Certificate Path Validation check on the SS1SPCA Certificates provided.

(d) If all verification checks are successful, the Secure SMETS1 Device stores the SS1SPCA Certificate chain and its own SS1SP End Entity Certificate in its internal storage.

14.6 SS1SP PKI Personnel RA verification and issuance of certificate

(A) Only authorised SS1SPCA Personnel (in accordance with Part 3.2.3 of the Policy) are granted a Privileged Role allowing them to create Certificate Requests, approve Certificate Requests and Issuing Certificates in accordance with this procedure and in accordance with the Policy:

(i) A service request is raised by the Service Team for issuance of a SS1SP End Entity Certificate as outlined in Part 3.3.1 (B) of the Policy;

(ii) A CSR is generated by SS1SPCA Personnel using the SS1SPCA CSR Generation Tool;

(iii) The SS1SPCA Personnel who generated the CSR then submits the CSR to the SS1SPCA Management Tool;

(iv) The SS1SPCA Management Tool parses the CSR in order to display the content of the CSR (including Subject information);

(v) The SS1SPCA Personnel who submitted the CSR verifies the contents of the CSR output and:

  (a) If successful, confirms the Certificate issuance through the SS1SPCA Management Tool;

  (b) The SS1SPCA Personnel then export the Certificate in PKCS#7 format file from SS1SPCA Management Tool; or

  (c) If unsuccessful, the SS1SPCA Personnel rejects the Certificate and starts the process again from Part 14.6 (A)(i) of this Annex E of the Policy;

(vi) This PKCS#7 file containing the Certificate is loaded back into the SS1SPCA CSR Generation Tool by the SS1SPCA Personnel;

(vii) The SS1SPCA CSR Generation Tool then verifies the PKCS#7 file including the issued SS1SP End Entity Certificate and the SS1SPCA Certificate chain within the PKCS#7 file, and:

  (a) If the PKCS#7 file validates successfully, the SS1SPCA CSR Generation Tool creates a PKCS#12 file ready for download by SS1SPCA Personnel. This file contains both the SS1SP End Entity Private Key associated with Public Key in the SS1SP End Entity Certificate and the complete SS1SPCA Certificate chain;

  (b) The SS1SPCA Personnel download the PKCS#12 file and then load into the appropriate System accordingly; or

  (c) If the PKCS#7 file cannot be validated successfully, the PKCS#7 file is rejected by the SS1SPCA Personnel and the process starts again.

Version 3.0

Appendix AP2

S1SPKI Certificate Policy

FOC S1SPKI Certificate Policy

FOC S1SPKI Certificate Policy

1 INTRODUCTION

The document comprising of this Final Operating Capacity SMETS1 Service Provider Certificate Policy together with its Annexes, shall be known as the “FOC S1SPKI Certificate Policy” (and this document is referred to simply as the “Policy”).

1.1 Overview

(A) This Policy sets out the arrangements of the FOC S1SPKI related to the issuance of the following Certificates:

(i) FOC SISPKI End Entity Certificates; and

(B) FOC S1SPKI CA Certificates. This Policy is structured according to the guidelines provided by IETF RFC 3647, with appropriate extensions, modifications and deletions.

(C) Except where the context otherwise requires, words or expressions used in this Policy shall have the meanings ascribed to them in IETF RFC 5280 where they:

(i) appear in `Courier New font`;

(ii) are accompanied by the descriptor 'field', 'type' or 'extension'; and/or

(iii) take the form of a conjoined string of two or more words, such as '`digitalSignature`'.

Where in this Policy, a system or device is expressed to be a Registration Authority, a FOC S1SPKI CA, an Authorised Subscriber, Subscriber or a Relying Party, this shall be interpreted as meaning that the DCC Service Provider operating the relevant system or device is the Registration Authority, the Certification Authority, Authorised Subscriber, Subscriber or Relying Party (as the case may be). In the case of any SMETS1 Device, the FOC S1SP shall be the Authorised Subscriber and/or Relying Party (as the case may be).

1.2 Document name and identification

(A) This Policy has not been assigned an OID.

1.3 FOC S1SPKI participants

1.3.1 FOC S1SPKI CA

(A) The definition of FOC S1SPKI CA can be found in Annex A.

1.3.2 FOC S1SPKI Registration Authority

(A) The definition of FOC S1SPKI Registration Authority can be found in Annex A.

1.3.3 Subscribers

(A) In accordance with the FOC S1SPKI RAPP as set out in Annex E of this Policy, certain Parties may become Authorised Subscribers.

(B) In accordance with the FOC S1SPKI RAPP as set out in Annex E of this Policy an Authorised Subscriber shall be an Eligible Subscriber in relation to certain Certificates.

(C) The FOC S1SPKI RAPP as set out in Annex E of this Policy sets out the procedure to be followed by an Eligible Subscriber in order to become a Subscriber for one or more Certificates.

(D) Eligible Subscribers are subject to the applicable requirements of the FOC S1SPKI RAPP as set out in Annex E of this Policy and Subscriber Obligations as set out in Annex C this Policy.

(E) The definitions of the following terms are set out in Annex A of this Policy:

(i) Authorised Subscriber;

(ii) Eligible Subscriber;

(iii) Subscriber.

1.3.4 Subjects

(A) The Subject of a FOC S1SPKI End Entity Certificate is represented by an appropriate identifier in the subject field of the FOC S1SPKI End Entity Certificate Profile (as the case may be) in accordance with Annex B.

(B) The Subject of a FOC S1SPKI CA Certificate must be the entity identified by the subject field of the FOC S1SP Operator Root CA Certificate Profile, the Intermediate Enterprise CA Certificate Profile; the Intermediate Operator CA Certificate Profile; the Application Service Root CA Certificate Profile or the Intermediate Application Service PKI CA Certificate Profile (as the case may be) in accordance with Annex B.

(C) The definition of Subject is set out in Annex A.

1.3.5 Relying Parties

(A) In accordance with this Policy, certain Parties may be Relying Parties.

(B) Relying Parties are subject to the applicable requirements of the Relying Party Obligations as set out in Annex D of this Policy.

(C) The definition of Relying Party is set out in Annex A.

1.3.6 Policy Management Authority

(A) The FOC S1SP’s IT Steering Committee (FOC S1SP ITSC) is responsible for fulfilling the duties of the Policy Management Authority in relation to the FOC S1SPKI.

(B) This Policy is subject to periodic review by the SMKI PMA in accordance with the provisions of the SEC.

1.3.7 FOC S1SPKI Repository

(A) The FOC S1SPKI CA will be responsible for providing the FOC S1SPKI Repository in accordance with this Policy.

1.3.8 Certificate usage

(A) The FOC S1SP Intermediate CA shall ensure that FOC S1SP End Entity Certificates are Issued only:

(i) to Eligible Subscribers; and

(ii) for the purposes of:

a) the creation, sending, receipt and processing of communications to and from FOC SMETS1 Devices in accordance with or pursuant to the Smart Energy Code (SEC), which will further include:

1) Symmetric key generation (Digital Signature, Key Agreement);

2) TLS Communication (Digital Signature, Key Agreement, TLS Web Client Authentication, TLS Web Server Authentication); and

3) Authentication and Non-Repudiation (Digital Signature, Non-Repudiation, Key Encipherment, Data Encipherment, Key Agreement, TLS Web Client Authentication, TLS Web Server Authentication).

(B) The FOC S1SPCA shall ensure that FOC S1SPCA Certificates are Issued only to the FOC S1SPCA:

(i) in its capacity as, and for the purposes of exercising the functions of, the FOC S1SP Operator Root Certification Authority (CA);

(ii) in its capacity as, and for the purposes of exercising the functions of, the Intermediate Enterprise CA; and

(iii) in its capacity as, and for the purposes of exercising the functions of, the Intermediate Operator CA.

(C) The Intermediate Application Service PKI CA shall ensure that Application Service End Entity Certificates are Issued only:

(ii) to Eligible Subscribers; and

(iii) for the purpose of secure communications and authenticating users to the Application Service for administration purposes.

(D) The Further provision in relation to the use of Certificates is made in the Subscriber Obligations as set out in Annex C of this Policy and the Relying Party Obligations as set out in Annex D of this Policy.

1.3.9 Prohibited Certificate uses

(A) No party shall use a Certificate other than for the purposes specified in Part 1.3.8 of this policy.

1.4 Policy administration

1.4.1 Organisation administering the document

(A) This Policy is a SEC Subsidiary Document and is administered as such in accordance with the provisions of the Code.

1.4.2 Contact person

(A) Questions in relation to the content of this Policy should be addressed to the Chief Information Security Officer CISO at DCC.

1.4.3 Person determining CPS suitability for the policy

(A) The SMKI PMA determines the suitability of any Certification Practice Statement operating under this Policy.

1.4.4 CPS approval procedures

(A) The FOC S1SPKI CPS is subject to a review by, the SMKI PMA in accordance with the provisions of the SEC.

(B) The DCC shall keep the FOC S1SPKI CPS under review and shall in particular carry out a review of the FOC S1SPKI CPS whenever (and to the extent to which) it may be required to do so in line with its duties as set out in the SEC.

(C) Following any review of the FOC S1SPKI CPS:

(i) the FOC S1SP may propose amendments to it, which it shall submit to the SMKI PMA for its review; and

(ii) those amendments may be made only to the extent to which the SMKI Policy Management Authority has approved or not rejected them.

1.4.5 Registration Authority Policies and Procedures

(A) The FOC S1SPKI Registration Authority Policies and Procedures (the FOC S1SPKI RAPP) are set out in Annex E of this Policy.

1.5 Definitions and acronyms

(A) Definitions of the expressions used in this Policy are set out in Section A of the Code (Definitions and Interpretation) and Annex A of this Policy.

(B) Any acronyms used for the purposes of this Policy are set out in Section A of the Code (Definitions and Interpretation) and Annex A of this Policy.

2 PUBLICATION AND REPOSITORY RESPONSIBILITIES

2.1 FOC S1SPKI Repositories

(A) The FOC S1SPKI Operator Root CA and the FOC S1SPKI Intermediate CAs each have their own separate FOC S1SPKI Repository.

(B) The FOC S1SPKI Repository associated with the FOC S1SPKI Operator Root CA stores the following information:

(i) All copies of Issued FOC S1SPKI Operator Root CA Certificates

(ii) Certificate status and validity meta-data for each FOC S1SPCA Certificate

(C) The FOC S1SPKI Repository associated with the FOC S1SPKI Intermediate CAs shall store the following information:

(i) All copies of FOC S1SP End Entity Certificates Issued by the FOC S1SPKI Intermediate CAs.

(ii) Certificate status and validity meta-data for each FOC S1SP End Entity Certificate Issued by the FOC S1SPKI Intermediate CAs.

(iii) The latest version of the FOC S1SPKI CRL for the FOC S1SPKI Intermediate CAs.

(iv) All copies of Issued FOC S1SP CA Certificates.

(D) The FOC S1SPKI Repository associated with each of the individual Application Service Root CAs shall store the following information:

(i) All copies of the Application Service Root CA Certificate self-signed by that Application Service Root CA

(ii) All copies of Intermediate Application Service PKI CA Certificates Issued by that Application Service Root CA

(iii) All copies of Application Service End Entity Certificates Issued by the Intermediate Application Service PKI CA referred to in ii) above;

(iv) Certificate status and validity meta-data for each of the Application Service End Entity Certificates stored in that repository.

2.2 Publication of certification information

(A) See part 2.1 of this Policy.

2.3 Time or frequency of publication

(A) The FOC S1SPKI CA shall ensure that:

(i) each FOC S1SPKI End Entity Certificate is promptly accepted by a Subscriber when issued;

(ii) each FOC S1SPKICA Certificate is lodged in the applicable FOC S1SPKI Repository promptly on being Issued;

(iii) the FOC S1SPKI ARL is lodged in the FOC S1SPKI Repository, and a revised version of the FOC S1SPKI ARL is lodged in the FOC S1SPKI Repository within such time as is specified in Part 4.9.6 of this Policy; and

(iv) the FOC S1SPKI CRL is lodged in the FOC S1SPKI Repository, and a revised version of the FOC S1SPKI CRL is lodged in the FOC S1SPKI Repository within such time as is specified in Part 4.9.6 of this Policy.

(B) The Applications Service CA shall ensure that:

(i) each Application Service End Entity Certificate is promptly accepted by a Subscriber when issued;

(ii) each Application Service CA Certificate is lodged in the applicable Application Service Repository promptly on being Issued;

(iii) the FOC S1SPKI ARL is lodged in the FOC S1SPKI Repository, and a revised version of the FOC S1SPKI ARL is lodged in the FOC S1SPKI Repository within such time as is specified in Part 4.9.6 of this Policy; and

(iv) the FOC S1SPKI CRL is lodged in the FOC S1SPKI Repository, and a revised version of the FOC S1SPKI CRL is lodged in the FOC S1SPKI Repository within such time as is specified in Part 4.9.6 of this Policy.

(C) No ARLs exist for the Application Service.

2.4 Access controls on FOC S1SPKI Repositories

(A) All FOC S1SPKI Repositories and Application Service Repositories are subject to access controls using username and passwords. Only authorised FOC S1SPKI Systems and FOC S1SP Personnel have access to FOC S1SPKI Repositories and Application Service Repositories.

3 IDENTIFICATION AND AUTHENTICATION

3.1 Naming

3.1.1 Types of names

(A) The FOC S1SPKI CA shall ensure that the name of the entity that is the Subject of each Certificate is in accordance with the relevant Certificate Profile at Annex B.

3.1.2 Need for names to be meaningful

(A) The FOC S1SPKI CA shall ensure that the name of the Subject of each Certificate is meaningful and consistent with the relevant Certificate Profile in Annex B.

3.1.3 Anonymity or pseudonymity of subscribers

(A) The anonymity or pseudonymity of Subscribers is not supported under this Policy.

3.1.4 Rules for interpreting various name forms

(A) Provision in relation to name forms is made in Annex B.

3.1.5 Uniqueness of names

(A) Provision in relation to the uniqueness of names is made in Annex B.

3.1.6 Recognition, Authentication, and role of trademarks

(A) No Eligible Subscriber may make a Certificate Signing Request which contains:

(i) any information that constitutes a trademark, unless it is the holder of the Intellectual Property Rights in relation to that trademark; or

(ii) any confidential information which would be contained in a Certificate Issued in response to that Certificate Signing Request.

3.2 Initial identity validation

3.2.1 Method to prove possession of Private Key

(A) Provision is made in the FOC S1SPKI RAPP as set out in Annex E of this policy in relation to:

(i) the procedure to be followed by an Eligible Subscriber in order to prove its possession of the Private Key which is associated with the Public Key to be contained in any Certificate that is the subject of a Certificate Signing Request; and

(ii) the procedure established for this purpose is in accordance with the procedure in PKCS#10 or an equivalent cryptographic mechanism.

3.2.2 Authentication of organisation identity

(A) Only Eligible Subscribers are allowed to subscribe for Certificates under this Policy.

3.2.3 Authentication of individual identity

(A) Provision is made in the FOC S1SPKI RAPP in relation to the Authentication of

(B) persons engaged by the FOC S1SP, which provides for all such persons to have their identity and authorisation verified to ISO27001 standards or to such equivalent level within a comparable authentication framework as may be agreed by the FOC S1SP ITSC.

3.2.4 Non-verified subscriber information

(A) The FOC S1SPKICA shall verify all information in relation to Certificates Issued.

(B) Further provision on the content of a Certificate is made in Subscriber Obligations as set out in Annex C of this Policy.

3.2.5 Validation of authority

(A) See part 3.2.2 of this Policy.

3.2.6 Criteria for interoperation

[*Not applicable in this Policy*]

3.3 Identification and Authentication for re-key requests

3.3.1 Identification and Authentication for routine re-key

(A) This Policy does not support Certificate Re-Key.

(B) The FOC S1SPKI CA shall not provide a Certificate Re-Key service.

3.3.2 Identification and Authentication for re-key after revocation

[Not applicable in this policy]

3.4 Identification and Authentication for revocation request

(A) Provision is made in the Annex E of this Policy in relation to procedures designed to ensure the Authentication of FOC S1SPKI RA Personnel who submit a Certificate Revocation Request and verify that they are authorised to submit that request.

(B) Only FOC S1SPKI RA Personnel can revoke a Certificate in accordance with Annex E of this Policy.

4 CERTIFICATE LIFE-CYCLE OPERATIONAL REQUIREMENTS

4.1 Certificate Application

4.1.1 Submission of Certificate Applications

(A) Provision is made in the FOC S1SPKI RAPP as set out in Annex E of this Policy in relation to:

(i) in respect of a FOC S1SPKI End Entity Certificate:

(a) the circumstances in which an Eligible Subscriber may submit a Certificate Signing Request; and

(b) the means by which it may do so, including through the use of an authorised System; and

(ii) in respect of a FOC S1SPKI CA Certificate, the procedure to be followed by an Eligible Subscriber in order to obtain a FOC S1SPCA Certificate.

4.1.2 Enrolment Process and Responsibilities

(A) Provision is made where applicable in the FOC S1SPKI RAPP as set out in Annex E of this Policy in relation to the:

(i) establishment of an enrolment process in respect of organisations, individuals, Systems and SMETS1 Devices in order to Authenticate them and verify that they are authorised to act on behalf of an Eligible Subscriber or Authorised Subscriber in its capacity as such; and

(ii) maintenance by the FOC S1SPKI CA of a list of organisations, individuals, Systems and SMETS1 Devices enrolled in accordance with that process.

4.1.3 Enrolment Process for the Registration Authorities and its Representatives

(A) Provision is made in the FOC S1SPKI RAPP as set out in Annex E of this Policy in relation to the establishment of an enrolment process in respect of FOC S1SP Personnel, FOC S1SPKI Systems and FOC S1SPKI RA Personnel:

(i) in order to Authenticate them and verify that they are authorised to act on behalf of the FOC S1SP in its capacity as the FOC S1SPKI Registration Authority; and

(ii) including in particular, for that purpose, provision:

(a) for Authentication of all FOC S1SPKI RA Personnel by a FOC S1SPKI Registration Authority Manager; and

(b) for all FOC S1SPKI Registration Authority Personnel to have their identify and authorisation verified against a robust assured authentication framework as agreed by the FOC S1SP ITSC. See section 6.3.2 of this Certificate Policy for further information.

4.2 Certificate application processing

4.2.1 Performing identification and Authentication functions

(A) Provision is made in the FOC S1SPKI RAPP in relation to the Authentication by the FOC S1SPKI CA of Eligible Subscribers which submit a Certificate Signing Request.

4.2.2 Approval or rejection of Certificate applications

(A) Where any Certificate Signing Request fails to satisfy the requirements set out in the FOC S1SPKI RAPP as set out in Annex E of this Policy or this Policy, the FOC S1SPKI CA:

(i) shall reject it and refuse to Issue the Certificate which was the subject of the Certificate Signing Request; and

(ii) may give notice to the Party which made the Certificate Signing Request of the reasons for its rejection.

(B) Where any Certificate Signing Request satisfies the requirements set out in the FOC S1SPKI RAPP as set out in Annex E of this Policy or any other provision of this Policy, the FOC S1SPKI CA shall Issue the Certificate which was the subject of the Certificate Signing Request.

(C) This does not apply in circumstances where a Certificate is issued by a System to another System or device.

4.2.3 Time to process Certificate applications

(A) All Certificate Signing Requests will be processed promptly upon receipt.

(B) Upon receipt and successful validation of a Certificate Signing Request by the FOC S1SPKI CA, the FOC S1SPKI CA will promptly Issue a Certificate in response.

4.3 Certificate issuance

4.3.1 FOC S1SPCA Actions during Certificate Issuance

(A) The FOC S1SPKI CA may Issue a Certificate only:

(i) in accordance with the provisions of this Policy and the FOC S1SPKI RAPP as set out in Annex E of this Policy; and

(ii) in response to a Certificate Signing Request made by an Eligible Subscriber in accordance with the FOC S1SPKI RAPP as set out in Annex E of this Policy.

(B) The FOC S1SPKI CA shall ensure that:

(i) each FOC S1SPKI CA Certificate Issued by it contains information that it has verified to be correct and complete; and

(ii) each FOC S1SPKI End Entity Certificate Issued by it contains information consistent with the information in the Certificate Signing Request.

(C) A FOC S1SPCA Certificate may only be:

(i) Issued by the FOC S1SPCA; and

(ii) for that purpose, self-signed using the Operator Root CA Private Key for the Operator Root CA Certificate and signed using the Operator Root CA Private Key for a FOC S1SP Intermediate CA Certificate.

(D) A FOC S1SP End Entity Certificate may only be:

(i) Issued by an FOC S1SP Intermediate CA; and

(ii) for that purpose, signed using a FOC S1SP Intermediate CA Private Key.

(E) The FOC S1SPCA shall not Issue:

(i) an FOC S1SP Intermediate CA Certificate using an Operator Root CA Private Key after the expiry of the Validity Period of an Operator Root CA Certificate containing the Public Key associated with that Private Key;

(ii) an FOC S1SP End Entity Certificate using an FOC S1SP Intermediate CA Private Key after the expiry of the Validity Period of an FOC S1SP Intermediate CA Certificate containing the Public Key associated with that Private Key; or

(iii) any Certificate containing a Public Key where it is aware that the Public Key is the same as the Public Key contained in any other Certificate that was previously Issued by it.

(F) An Application Service CA Certificate may only be:

(i) Issued by the Application Service CA; and

(ii) for that purpose, self-signed using the Application Service Root CA Private Key for an Application Service Root CA Certificate and signed using the Application Service Root CA Private Key for an Intermediate Application Service PKI Certificate.

(G) An Application Service End Entity Certificate may only be:

(i) Issued by an Intermediate Application Service CA; and

(ii) for that purpose, signed using an Application Service Intermediate PKI CA Private Key.

(H) The Application Service CA shall not Issue:

(i) an Intermediate Application Service PKI CA Certificate using an Application Service Root CA Private Key after the expiry of the Validity Period of an Applications Service Root CA Certificate containing the Public Key associated with that Private Key;

(ii) an Application Service End Entity Certificate using an Intermediate Application Service PKI CA Private Key after the expiry of the Validity Period of an Application Service Intermediate PKI CA Certificate containing the Public Key associated with that Private Key; or

(iii) any Certificate containing a Public Key where it is aware that the Public Key is the same as the Public Key contained in any other Certificate that was previously Issued by it.

4.3.2 Notification to subscriber by the CA of issuance of Certificate

(A) Provision is made in the FOC S1SPKI RAPP as set out in Annex E of this Policy for the FOC S1SP CA to notify an Eligible Subscriber where that Eligible Subscriber is issued with a Certificate which was the subject of a Certificate Signing Request made by it.

(B) This does not apply in circumstances where a Certificate is issued by a System to another System or device.

4.4 Certificate Acceptance

4.4.1 Conduct constituting Certificate acceptance

(A) A Certificate which has been Issued by the FOC S1SPKI CA shall be treated as valid for any purposes of this Policy or the Code until it is revoked.

(B) The FOC S1SPKI CA shall maintain a record of all Certificates which have been Issued by it and are treated as accepted by a Subscriber.

4.4.2 Publication of the Certificate by the CA

(A) Provision in relation to publication of Certificates is made in Part 2 of this Policy.

4.4.3 Notification of Certificate issuance by the CA to other entities

(A) Not applicable in this Policy.

4.5 Key Pair and Certificate Usage

4.5.1 Subscriber Private Key and Certificate Usage

(A) Provision for restrictions on the use by Subscribers of Private Keys in respect of Certificates is made in this Policy.

4.5.2 Relying Party Public Key and Certificate usage

(A) Relying Party obligations are set out in Annex D of this Policy.

4.6 Certificate Renewal

4.6.1 Circumstance for Certificate Renewal

(A) This policy does not support the renewal of Certificates.

(B) The FOC S1SPKI CA may only replace and shall not renew any Certificate.

4.6.2 Who may request replacement

(A) Certificate replacement is an automated process and does not require manual intervention. The business process defines the rotation schedule of the certificate Processing Certificate replacement requests.

(B) Certificate Replacement operates under the governance of the Head End System. In its capacity as the Registration Authority it determines whether a Certificate needs to be issued and manages the creation of the CSR.

4.6.3 Notification of new Certificate issuance to subscriber

Not applicable to this Policy.

4.6.4 Conduct constituting acceptance of a replacement Certificate

Not applicable to this Policy.

4.6.5 Publication of the replacement Certificate by the CA

Not applicable to this Policy.

4.6.6 Notification of Certificate issuance by the CA to other entities

Not applicable to this Policy.

4.7 Certificate re-key

4.7.1 Circumstance for Certificate re-key

(A) This Policy does not support Certificate Re-Key.

4.7.2 Who may request certification of a new public key

Not applicable to this policy.

4.7.3 Processing Certificate re-keying requests

Not applicable to this policy.

4.7.4 Notification of new Certificate issuance to subscriber

Not applicable to this policy.

4.7.5 Conduct constituting acceptance of a re-keyed Certificate

Not applicable to this policy.

4.7.6 Publication of the re-keyed Certificate by the CA

Not applicable to this policy.

4.7.7 Notification of Certificate issuance by the CA to other entities

Not applicable to this policy.

4.8 Certificate modification

4.8.1 Circumstance for Certificate modification

(A) This policy does not support Certificate modification.

4.8.2 Who may request Certificate modification

Not applicable to this policy.

4.8.3 Processing Certificate modification requests

Not applicable to this policy.

4.8.4 Notification of new Certificate issuance to subscriber

Not applicable to this policy.

4.8.5 Conduct constituting acceptance of modified Certificate

Not applicable to this policy.

4.8.6 Publication of the modified Certificate by the CA

Not applicable to this policy.

4.8.7 Notification of Certificate issuance by the CA to other entities

Not applicable to this policy.

4.9 Certificate Revocation and Suspension

(A) This Policy does not support Certificate suspension.

(B) Certificate status information services shall identify all revoked Certificates; at least until their assigned validity period expires. A reporting API describes the status of a Certificate at a CRL Distribution Point (CDP) and can be queried by a Privileged User.

4.9.1 Circumstances for Revocation

(A) A Subscriber shall ensure that it submits a Certificate Revocation Request in relation to a Certificate in accordance with Annex E of this policy where:

- (i) immediately upon becoming aware that the Certificate has been Compromised, or is suspected of having been Compromised; or
- (ii) immediately upon ceasing to be an Eligible Subscriber in respect of that Certificate

(B) A Certificate must be Revoked:

(i) When any of the information in the Certificate is known or suspected to be inaccurate.

(ii) Upon suspected or known compromise of the Private Key associated with the Certificate.

(iii) Upon suspected or known compromise of the media holding the Private Key associated with the Certificate.

(C) The FOC S1SPKI CA, or FOC S1SPKI RA acting on their behalf may Revoke a Certificate when an entity fails to comply with any obligations set out in this Policy.

(D) Handshake information describing the exchange of information for revocation purposes can be obtained in section 2.3 'Operator Device Certificate Update' of the DCCA-0045-VN.N-SDD Trilliant S1SP WAN communication Security' documentation.

4.9.2 Who can request revocation

(A) Any Subscriber may submit a Certificate Revocation Request in relation to a Certificate for which it is the Authorised Subscriber and shall on doing so by specifying its reason for submitting the Certificate Revocation Request (which shall be a reason consistent with Part 4.9.1 of this Policy).

4.9.3 Procedure for revocation request

(A) Provision is made in the FOC S1SPKI RAPP in relation to the procedure for submitting and processing a Certificate Revocation Request.

(B) On receiving a Certificate Revocation Request, the FOC S1SPKI CA shall take reasonable steps to:

(i) Authenticate the Subscriber making that request;

(ii) Authenticate the Certificate to which the request relates; and

(iii) confirm that a reason for the request has been specified in accordance with Part 4.9.2 of this Policy.

(C) The FOC S1SPKI CA shall inform the Subscriber for a Certificate where that Certificate has been revoked.

4.9.4 Revocation request grace period

(A) None. If the Revocation request is actioned, it must reflect in the next scheduled publication of the CRL.

4.9.5 Time within which CA must process the revocation request

(A) The FOC S1SPKI CA shall ensure that it processes all Certificate Revocation Requests promptly, and in any event in accordance with such time as is specified in the FOC S1SPKI RAPP.

(B) The mechanisms, if any, that a Relying Party may use in order to check the Certificate Status Information of the Certificate upon which they wish to rely, must be via Certificate Revocation Lists or equivalent on-line protocol that permits authenticity and integrity of the Status Information to be verified

4.9.6 CRL issuance frequency (if applicable)

(A) The FOC S1SPKI CA shall ensure that an up to date version of the FOC S1SPKI ARL is lodged in the FOC S1SPKI Repository:

(i) at least once in every period of twelve months; and

(ii) promptly on the revocation of an FOC S1SPCA Certificate.

(B) Each version of the FOC S1SPKI ARL shall be valid until the date which is up to 13 months after the date on which that version of the FOC S1SPKI ARL is lodged in the FOC S1SPKI Repository.

(C) Further provision in relation to the reliance that may be placed on the FOC S1SPKI ARL (and on versions of it) is set out in Annex D (Relying Party Agreement) of this Policy.

(D) The FOC S1SPCA shall ensure that an up to date version of the FOC S1SPKI CRL is lodged in the relevant FOC S1SPKI Repository at least once in every period of 48 hours.

(E) Each version of the FOC S1SPKI CRL shall be valid until 48 hours from the time at which it is lodged in the FOC S1SPKI Repository.

(F) Further provision in relation to the reliance that may be placed on the FOC S1SPKI CRL (and on versions of it) is set out in Annex D (Relying Party Agreement) of this Policy.

(G) The FOC S1SPCA shall ensure that each up to date version of the FOC S1SPKI ARL and FOC S1SPKI CRL:

  (i) continues to include each relevant revoked Certificate until such time as the Validity Period of that Certificate has expired; and
  (ii) does not include any revoked Certificate after the Validity Period of that Certificate has expired.

(H) The FOC S1SPCA shall ensure that the FOC S1SPKI CRL contains a non-critical entry extension which identifies the reason for the revocation of each Certificate listed on it in accordance with RFC 5280 (section 5.3.1).

(I) The FOC S1SPCA shall retain a copy of the information contained in all versions of the FOC S1SPKI CRL and FOC S1SPKI ARL, together with the dates and times between which each such version was valid. This information shall be made available as soon as is reasonably practicable, on receipt of a request, to the DCC, the FOC ,FOC S1SP ITSC any Subscriber or any Relying Party.

(J) No ARL or CRL is issued in relation to the Internal Application Service CA.

4.9.7 Maximum latency for CRLs (if applicable)

(A) See part 4.9.6 of this Policy

4.9.8 On-line revocation/status checking availability

(A) The availability of Certificate Status checking shall be published though a CRL Distribution Points (CDP).

4.9.9 On-line revocation checking requirements

(A) See section 4.9.8 above

4.9.10 Other forms of revocation advertisements available

[*Not applicable in this Policy*]

4.9.11 Special requirements in the event of key compromise

(A) Where any Private Key is Compromised, then the FOC S1SP shall:

  (i) immediately notify the SMKI PMA;
  (ii) provide the SMKI PMA with all of the information known to it in relation to the nature and circumstances in the event of Compromise or suspected Compromise; and
    (a) where the Compromise or suspected Compromise relates to any Private Key;
  (iii) ensure that the Private Key is no longer used;
  (iv) promptly notify each of the Authorised Subscribers for any Certificates Issued using that Private Key.

4.9.12 Circumstances for suspension

4.9.13 Who can request suspension

[*Not applicable in this Policy*]

4.9.14 Procedure for suspension request

[Not applicable in this Policy]

4.9.15 Limits on suspension period

[Not applicable in this Policy]

4.10 Certificate status services

4.10.1 Operational characteristics

(A) The types of Certificate status checking services made available to the Authorised Subscriber is by a service endpoint. This service endpoint is available to the Authorised Subscriber as an application interface which is presented by the PKI software.

4.10.2 Service availability

(A) See part 4.9.6 of this Policy.

4.11 End of subscription

[Not applicable in this Policy].

4.12 Key escrow and recovery

4.12.1 Key escrow and recovery policy and practices

(A) This Policy does not cover Key Escrow services.
(B) The FOC S1SPKI CA shall not provide any Key Escrow services.
(C) The FOC S1SPKI recovery policies and practices are documented in the FOC S1SPKI CPS

4.12.2 Session key encapsulation and recovery policy and practices

[Not applicable in this Policy]

5 FACILITY, MANAGEMENT, AND OPERATIONAL CONTROLS

(A) The FOC S1SP shall ensure that the FOC S1SPKI CPS incorporates detailed provision in relation to the facility, management, and operational controls to be established and operated for the purposes of the exercise of its functions as the FOC S1SPKI CA.

5.1 Physical controls

5.1.1 Site location and construction

(A) The FOC S1SP shall ensure that all Data Centres must be located in List X Site accredited sites and must be ISO27001 certified.

(B) The FOC S1SP shall ensure that the FOC S1SPKI Systems are operated in a sufficiently secure environment, which shall at least satisfy the requirements set out at Section G2 (System Security: Obligations on the DCC) and Section G5 (Information Security: Obligations on the DCC and Users) of the Code.

(C) The FOC S1SP shall ensure that:

- (i) all of the physical locations in which the FOC S1SPKI Systems are situated, operated, routed or directly accessed are in the United Kingdom;
- (ii) all bespoke Security Related Functionality is developed, specified, designed, built and tested only within the United Kingdom; and
- (iii) all Security Related Functionality is integrated, configured, tested in situ, implemented, operated and maintained only within the United Kingdom.

(D) The FOC S1SP shall ensure that the FOC S1SPKI Systems cannot be indirectly accessed from any location outside the United Kingdom.

(E) The FOC S1SP shall ensure that the FOC S1SPKI CPS incorporates provisions designed to ensure that all physical locations in which the manufacture of Certificates and Time-Stamping take place are at all times manually or electronically monitored for unauthorised intrusion in accordance with:

- (i) SMKI PMA and SSC Guidance (Standards, Procedures and Guidelines) on Protective Monitoring; or
- (ii) any equivalent to the SMKI PMA and SSC Guidance (Standards, Procedures and Guidelines) on Protective Monitoring which updates or replaces it from time to time.

(F) The FOC S1SP shall ensure that the FOC S1SPKI CPS incorporates provisions designed to ensure that all PINs, passphrases and passwords used for the purposes of carrying out the functions of the FOC S1SPCA are stored in secure containers accessible only to appropriately authorised individuals.

(G) The FOC S1SP shall ensure that the FOC S1SPKI Systems are Separated from any other DCC Systems provided that the FOC S1SPCA systems does not need to be Separated from the Application Service CA Systems

5.1.2 Physical access

(A) The FOC S1SP shall ensure that the FOC S1SPKI CPS incorporates provisions in relation to access control, including in particular provisions designed to:

- (i) establish controls such that only appropriately authorised personnel may have unescorted physical access to FOC S1SPKI Systems, or any System used for the purposes of Timestamping, Certificate generation, or Certificate life-cycle management;
- (ii) ensure that any unauthorised personnel may have physical access to such Systems only if appropriately authorised and supervised;
- (iii) ensure that a site access log is both maintained and periodically inspected for all locations at which such Systems are sited; and
- (iv) ensure that all removable media which contain sensitive plain text Data and are kept at such locations are stored in secure containers accessible only to appropriately authorised individuals.

5.1.3 Power and air conditioning

(A) The FOC S1SP shall ensure that the FOC S1SPKI CPS incorporates provisions in relation to power and air conditioning at all physical locations in which the FOC S1SPKI Systems are situated.

5.1.4 Water exposures

(A) The FOC S1SP shall ensure that the FOC S1SPKI CPS incorporates provisions in relation to water exposure at all physical locations in which the FOC S1SPKI Systems are situated.

5.1.5 Fire prevention and protection

(A) The FOC S1SP shall ensure that the FOC S1SPKI CPS incorporates provisions in relation to fire prevention and protection at all physical locations in which the FOC S1SPKI Systems are situated.

5.1.6 Media storage

(A) The FOC S1SP shall ensure that the FOC S1SPKI CPS incorporates provisions designed to ensure that appropriate controls are placed on all media used for the storage of Data held by it for the purposes of carrying out its functions as the FOC S1SPKI CA.

5.1.7 Waste disposal

(A) The FOC S1SP shall ensure that the FOC S1SPKI CPS incorporates provisions designing to ensure all media used to store Data held by it for the purposes of carrying out its functions as the FOC S1SPKI CA are disposed of only using secure methods. Where such methods such be based on:

(i) Information Assurance Standard No. 5:2011 (Secure Sanitisation);

(ii) any equivalent to that Information Assurance Standard which updates or replaces it from time to time; or

(iii) any equivalent standard or secure method approved by the FOC S1SP ITSC.

5.1.8 Off-Site Back-Up

(A) The FOC S1SP shall ensure that Capgemini and DXC shall regularly carry out a Back-Up of:

(i) all Data held on the S1SPKI Systems which are critical to the operation of those Systems or continuity in the provision of the S1SPKI Services; and

(ii) all other sensitive Data.

(B) The FOC S1SP shall ensure that Capgemini and DXC ensure that Data which are Backed-Up in accordance with paragraph (A):

(i) are stored on media that are located in physically secure facilities in different locations to the sites at which the Data being Backed-Up are ordinarily held;

(ii) are protected in accordance with the outcome of a risk assessment, including when being transmitted for the purposes of Back-Up; and

(iii) to the extent to which they comprise S1SPKI Private Key Material, are

(iv) Backed Up to appropriate Security Containers which are stored off-line in encrypted format.

(C) The FOC S1SP shall ensure that Capgemini and DXC ensure that, where any elements of the S1SPKI Systems, any Data held for the purposes of providing the SS1SP PKI Services, or any items of Capgemini and DXC equipment are removed from their primary location, they continue to be protected in accordance with the security standard appropriate to the primary location.

(D) DCC will ensure that the S1SPKI CPS incorporates provisions in relation to paragraphs (A), (B) and (C) above.

5.2 Procedural Controls

5.2.1 Trusted Roles

(A) The FOC S1SP shall ensure that:

(i) no individual may carry out any activity which involves access to resources, or Data held on, the FOC S1SPKI Systems unless that individual has been expressly authorised to have such access;

(ii) each member of FOC S1SPKI Personnel and FOC S1SPKI RA Personnel has a clearly defined level of access to the FOC S1SPKI Systems and the premises in which they are located;

(iii) no individual member of FOC S1SPKI Personnel or FOC S1SPKI RA Personnel is capable, by acting alone, of engaging in any action by means of which the FOC S1SPKI Systems may be Compromised to a material extent; and

(iv) the FOC S1SPKI CPS incorporates provisions designed to ensure that appropriate controls are in place for the purposes of compliance by the FOC S1SPKI CA with the requirements of this Part 5.2.1 of this Policy.

5.2.2 Number of persons required per task

(A) The FOC S1SP shall ensure that the FOC S1SPKI CPS incorporates provisions designed to establish:

(i) the appropriate separation of roles between the different members of FOC S1SPKI Personnel, FOC S1SPKI RA Personnel; and

(ii) the application of controls to the actions of all members of FOC S1SPKI Personnel or FOC S1SPKI RA Personnel who are Privileged Users, in particular:

(a) identifying any controls designed to ensure that the involvement of more than one individual is required for the performance of certain functions; and

(b) providing that the revocation of any Certificate is one such function.

(B) The FOC S1SP shall ensure that the FOC S1SPKI CPS, as a minimum, makes provision for the purposes of paragraph (A) in relation to the following areas:

(i) S1SPKI Systems administration;

(ii) S1SPKI Systems operations;

(iii) S1SPKI Systems security; and

(iv) S1SPKI Systems auditing.

5.2.3 Identification and Authentication for each role

(A) See Part 5.2.2 of this Policy.

5.2.4 Roles requiring separation of duties

(A) See Part 5.2.2 of this Policy.

5.3 Personnel controls

5.3.1 Qualifications, experience, and clearance requirements

(A) The FOC S1SP shall ensure that all FOC S1SPKI Personnel and FOC S1SPKI RA Personnel must:

(i) be appointed to their roles in writing;

(ii) be bound by contract to the terms and conditions relevant to their roles;

(iii) have received appropriate training with respect to their duties;

(iv) be bound by contract not to disclose any confidential, sensitive, personal or security-related Data except to the extent necessary for the performance of their duties or for the purposes of complying with any requirement of law; and

(v) in so far as can reasonably be ascertained by the FOC S1SP, not have been previously relieved of any past assignment (whether for the FOC S1SP or any other person) on the grounds of negligence or any other failure to perform a duty.

(B) The FOC S1SP shall ensure that all FOC S1SPKI Personnel and FOC S1SPKI RA Personnel have, as a minimum, passed an industry recognised and assured security check before commencing their roles.

(C) For Privileged Users, these assured security checks may include additional checks.

(D) The FOC S1SP shall ensure that the FOC S1SPKI CPS, as a minimum, makes provision for the purposes of paragraph (B) and (C) above.

5.3.2 Background check procedures

(A) See Part 5.3.1 of this Policy.

5.3.3 Training requirements

(A) See Part 5.3.1 of this Policy.

5.3.4 Retraining frequency and requirements

(A) The FOC S1SP shall ensure that the FOC S1SPKI CPS incorporates appropriate provisions relating to the frequency and content of retraining and refresher training to be undertaken by members of FOC S1SPKI Personnel and FOC S1SPKI RA Personnel.

5.3.5 Job rotation frequency and sequence

(A) The FOC S1SP shall ensure that the FOC S1SPKI CPS incorporates appropriate provisions relating to the frequency and sequence of job rotations to be undertaken by members of FOC S1SPKI Personnel and FOC S1SPKI RA Personnel.

5.3.6 Sanctions for unauthorized actions

(A) The FOC S1SP shall ensure that the FOC S1SPKI CPS incorporates appropriate provisions relating to sanctions for unauthorised actions undertaken by members of FOC S1SPKI Personnel and FOC S1SPKI RA Personnel.

5.3.7 Independent contractor requirements

(A) In accordance with the provisions of the Code and this Policy, references to the FOC S1SP in this Policy include references to persons with whom the FOC S1SP contracts in order to secure performance of its obligations as the FOC S1SP.

5.3.8 Documentation supplied to personnel

(A) The FOC S1SP shall ensure that all FOC S1SPKI Personnel and FOC S1SPKI RA Personnel are provided with access to all documents relevant to their roles or necessary for the performance of their duties, including in particular:

(i) this Policy;
(ii) the FOC S1SPKI CPS; and
(iii) any supporting documentation, statutes, policies or contracts.

5.4 Audit logging procedures

5.4.1 Types of events recorded

(A) The FOC S1SP shall ensure that:

(i) the FOC S1SPKI Systems record all activity in an audit log;
(ii) the FOC S1SPKI CPS incorporates a comprehensive list of all events that are to be recorded in an audit log in relation to:
  (a) the activities of FOC S1SPKI Personnel and FOC S1SPKI RA Personnel;
  (b) the use of FOC S1SPKI equipment;
  (c) the use of (including both authorised and unauthorised access, and attempted access to) any premises at which functions of the FOC S1SPCA are carried out;
  (d) communications and activities that are related to the Issue of Certificates (in so far as not captured by the FOC S1SPKI Systems audit log); and
(iii) it records in an audit log all the events specified in paragraph (ii).

5.4.2 Frequency of processing log

(A) The FOC S1SP shall ensure that:

(i) the audit logging functionality in the FOC S1SPKI Systems is fully enabled at all times;
(ii) all FOC S1SPKI Systems activity recorded in the Audit Log is recorded in a standard format that is compliant with:

(a) British Standard BS 10008:2008 (Evidential Weight and Legal Admissibility of Electronic Information);

(iii) any equivalent to that British Standard which updates or replaces it from time to time; or

(iv) an equivalent standard format that is commensurate with the standard in (i) and has been approved by the FOC S1SP ITSC.

(B) It monitors the FOC S1SPKI Systems in compliance with:

(i) SMKI PMA Guidance on Protective Monitoring;

(ii) any equivalent to that SMKI PMA Guidance on Protective Monitoring which updates or replaces it from time to time; or

(iii) equivalent guidance that is commensurate with the guidance in (i) and which has been approved by the FOC S1SP ITSC.

(C) The FOC S1SP shall ensure that the FOC S1SPKI CPS incorporates provisions which specify:

(i) how regularly information recorded in the Audit Log is to be reviewed; and

(ii) what actions are to be taken by it in response to types of events recorded in the Audit Log.

(D) The FOC S1SP shall ensure that the FOC S1SPKI CPS incorporates provisions in relation to access to the Audit Log, providing in particular that:

(i) Data contained in the Audit Log must not be accessible other than on a read-only basis; and

(ii) access to those Data must be limited to those members of FOC S1SPKI Personnel or FOC S1SPKI RA Personnel who are performing a dedicated system audit role.

5.4.3 Retention period for audit log

(A) The FOC S1SP shall:

(i) Ensure that the FOC S1SPKI Systems retain their Audit Log so that it incorporates, on any given date, a record of all system events occurring during a period of at least twelve months prior to that date; and

(ii) ensure that a copy of the Audit Log incorporating a record of all system events occurring prior to the beginning of that period is archived in accordance with the requirements of Part 5.5 of this Policy.

5.4.4 Protection of audit log

(A) The SS1SPCA shall ensure that the FOC S1SPKI CPS incorporates appropriate provisions relating to:

(i) the extent to which the Audit Log is retained electronically, the Data stored in it cannot be accessed other than on a read-only basis, and are protected from unauthorised viewing, modification and deletion in accordance with:

(a) British Standard BS 10008:2008 (Evidential Weight and Legal Admissibility of Electronic Information);

(b) any equivalent to that British Standard which updates or replaces it from time to time; or

(c) an equivalent standard format that is commensurate with the standard in (i) and has been approved by the FOC S1SP ITSC; and

(ii) the extent to which the Audit Log is retained in non-electronic form, the Data stored in it are appropriately protected from unauthorised viewing, modification and destruction in order to ensure that their integrity is maintained for evidential purposes.

5.4.5 Audit log backup procedures

(A) The FOC S1SP shall ensure that the FOC S1SPKI CPS incorporates provisions in relation to its system for Audit Log backup procedures. This should include, as a minimum, provisions for:

(i) Data contained in the Audit Log to be backed up (or, to the extent that the Audit Log is retained in non-electronic form, are copied):

(a) on a daily basis; or

(b) if activity has taken place on the FOC S1SPKI Systems only infrequently, in accordance with the schedule for the regular Back-Up of the Data held on those Systems.

(B) All Data contained in the Audit Log which are Backed-Up are, during Back-Up:

(i) be held in accordance with the outcome of a risk assessment which is documented in the FOC SS1SPKI CPS; and

(ii) be protected to the same standard of protection as the primary copy of the Audit Log in accordance with Part 5.4.4 of this Policy.

5.4.6 Audit collection system (internal vs. external)

(A) The FOC S1SP shall ensure that the FOC S1SPKI CPS incorporates provisions in relation to its system for collecting Data for the purpose of populating the Audit Log. Notification to event-causing subject

(B) The FOC S1SP shall ensure that the FOC S1SPKI CPS incorporates provisions in relation to its notification of any person who is (or is responsible for any System which is) the direct cause of an event recorded in the audit log.

5.4.7 Vulnerability assessments

(A) Provision is made in the FOC S1SPKI CPS in relation to the carrying out of vulnerability assessments in respect of the FOC S1SPKI Systems.

5.5 Records archival

5.5.1 Types of records archived

(A) The SS1SPCA shall ensure that it archives:

(i) the Audit Log in accordance with Part 5.4 of this Policy;

(ii) its records of all Data submitted to it by Eligible Subscribers for the purposes of Certificate Signing Requests; and

(iii) any other Data specified in this Policy as requiring to be archived in accordance with this Part 5.5.

5.5.2 Retention period for archive

(A) Where there is a need to Archive Data, the FOC S1SP CA shall ensure that any Data which is to be Archived is retained in accordance with their Data Retention and Destruction Policy.

(B) Archived information is to be retained for a period of no less than 12 months

5.5.3 Protection of archive

(A) The FOC S1SP shall ensure that the FOC S1SPKI CPS incorporates the following provisions as to how Data held in its Archive are:

(i) protected against any unauthorised access;

(ii) adequately protected against environmental threats such as temperature, humidity and magnetism; and

(iii) incapable of being modified or deleted.

5.5.4 Archive backup procedures

(A) The FOC S1SP shall ensure that the FOC S1SPKI CPS incorporates provisions in relation to its procedures for the Back-Up of its Archive.

5.5.5 Requirements for time-stamping of records

(A) Provision in relation to Timestamping is made in Part 6.8 of this Policy.

5.5.6 Archive collection system (internal or external)

(A) The FOC S1SP shall ensure that the FOC S1SPKI CPS incorporates provisions in relation to its system for collecting Data for the purpose of populating the Archive.

5.5.7 Procedures to obtain and verify archive information

(A) The FOC S1SP shall ensure that:

(i) Data held in the Archive are stored in a readable format during their retention period; and

(ii) those Data remains accessible at all times during their retention period, including during any period of interruption, suspension or cessation of the SS1SPCA's operations.

(B) The FOC S1SP shall ensure that the FOC S1SPKI CPS incorporates provisions in relation to the periodic verification by the FOC S1SPKI CA of the Data held in the Archive.

5.6 Key changeover

(A) The FOC S1SP shall only ever Issue a new Certificate in relation to a new Certificate Signing Request, where it is submitted by an Eligible Subscriber in accordance with the requirements of the FOC S1SPKI RAPP and the relevant provisions of this Policy.

(B) A Key Pair will require changeover in accordance with their corresponding Certificate validity period set out in Part 6.3.2 of this Policy.

(C) The FOC S1SP shall ensure that any FOC S1SPKI CA Key Pair changeovers are managed so as to prevent any disruption to the provision of the FOC S1SPKI Services.

5.7 Compromise and disaster recovery

5.7.1 Incident and compromise handling procedures

(A) The FOC S1SP shall ensure that the FOC S1SPKI CPS incorporates a business continuity plan which shall be designed to ensure:

(i) continuity in, or (where there has been unavoidable discontinuity) the recovery of, the provision of the FOC S1SPKI Services in the event of any Compromise of the FOC S1SPKI Systems or major failure in the FOC S1SP processes; and

(ii) that priority is given to maintain continuity in, or to recovering the capacity for, the revocation of Certificates and the making available of an up to date FOC S1SPKI ARL and FOC S1SPKI CRL.

(B) The FOC S1SP shall ensure that the procedures set out in the business continuity plan are:

(i) compliant with ISO 22301 and ISO 27031 (or any equivalent to those standards which update or replace them from time to time); and

(ii) tested periodically, and in any event at least once in each year, in order to ensure that they are operationally effective.

(C) The FOC S1SP shall ensure that the FOC S1SPKI CPS incorporates provisions setting out the approach to be taken by it in circumstances in which it suspects (or has reason to suspect) that any FOC S1SPKI Private Key or any part of the FOC S1SPKI Systems is Compromised.

5.7.2 Computing resources, software, and/or data are corrupted

(A) The FOC S1SP shall ensure that the business continuity plan established in accordance with Part 5.7.1 of this Policy incorporates provisions setting out the steps to be taken in the event of any loss of or corruption to computing resources, software or Data.

5.7.3 Entity Private Key compromise procedures

(A) See Part 5.7.1 of this Policy.

5.7.4 Business continuity capabilities after a disaster

(A) The FOC S1SP shall ensure that the business continuity plan established in accordance with Part 5.7.1 of this Policy is designed to ensure the recovery of the provision of the FOC S1SPKI Services within not more than 48 hours of the occurrence of any event causing discontinuity.

5.8 CA or RA termination

[*Not applicable in this Policy*]

6 TECHNICAL SECURITY CONTROLS

(A) The FOC S1SP shall ensure that the FOC S1SPKI CPS incorporates detailed provision in relation to the technical controls to be established and operated for the purposes of the exercise of its functions as the FOC S1SPKI CA.

6.1 Key pair generation and installation

6.1.1 Key pair generation

(A) The FOC S1SP shall ensure that all FOC S1SPKI CPS incorporates detailed provision in relation to the FOC S1SPKI CA Key Pair generation, where all Key Pairs which it uses for the purposes of this Policy are generated:

- (i) in a protected environment compliant with FIPS 140-2 Level 3 (or any equivalent to that Federal Information Processing Standard which updates or replaces it from time to time);
- (ii) using multi-person control, such that no single Privileged Person is capable of generating any such Key Pair; and
- (iii) using random numbers which are such as to make it computationally infeasible to regenerate those Key Pairs even with knowledge of when and by means of what equipment they were generated.

(B) The FOC S1SPKI CA shall not generate any Key Pair other than a FOC S1SPKI CA Key Pair.

(C) The FOC S1SP shall ensure that all FOC S1SPKI CA Private Keys that are not required for continuous operational purposes will be encrypted and stored securely in an off-line security container which requires M of N to activate the FOC SS1SPKI CA Private Key when required.

6.1.2 Private Key delivery to Subscriber

(A) In accordance with Part 6.1.1(B) of this Policy, the FOC S1SPKI CA shall not generate any Private Key for delivery to a Subscriber.

6.1.3 Public Key delivery to Certificate issuer

(A) The FOC S1SP shall ensure that the FOC S1SPKI CPS or the FOC S1SPKI RAPP as the case may be, incorporates provisions:

- (i) in relation to the mechanism by which Public Keys of Subscribers are delivered to it for the purpose of the exercise of its functions as the FOC S1SPKI CA; and
- (ii) ensuring that the mechanism uses a recognised standard protocol such as PKCS#10.

6.1.4 FOC S1SPCA Public Key delivery to Relying Parties

(A) The FOC S1SP shall ensure that the FOC S1SPKI CPS incorporates provisions:

- (i) in relation to the manner by which each FOC S1SPKI CA Public Key is to be lodged in the relevant FOC S1SPKI Repository;
- (ii) designed to ensure that the FOC S1SPKI CA Public Keys are securely lodged in the FOC S1SPKI Repository in such a manner as to guarantee that their integrity is maintained; and
- (iii) ensuring that the mechanism uses a recognised standard protocol such as PKCS#10 where FOC SS1SPKI CA Public Keys are delivered direct to the Relying Party.

6.1.5 Key sizes

(A) The FOC S1SPKI CA and every Subscriber shall ensure that all Key Pairs which each of them may use for the purposes of this Policy are of the size and characteristics set out in Annex B of this Policy.

6.1.6 Public Key parameters generation and quality checking

(A) The FOC S1SPKI CA shall ensure that any Public Key used by it for the purposes of this Policy shall be of values and lengths that make the success of known attacks infeasible.

(B) Each Subscriber shall ensure that any Public Key used by it for the purposes of this Policy shall be of values and lengths that make the success of known attacks infeasible.

6.1.7 Key Usage purposes (as per X.509 v3 keyUsage field)

(A) The FOC S1SPKI CA shall ensure that each Certificate that is Issued by it has a `keyUsage` field in accordance with RFC5759 and RFC5280.

(B) The FOC S1SPKI CA shall ensure that each FOC S1SPKI End Entity Certificate that is Issued by it has a `keyUsage` of either:

(i) `digitalSignature`; or

(ii) `keyAgreement`.

(C) The FOC S1SPKI CA shall ensure that each FOC S1SPKI CA Certificate that is Issued by it has a `keyUsage` of either:

(i) `keyCertSign`; or

(ii) `CRLSign`.

(D) The FOC S1SPKI CA shall ensure that no `keyUsage` values may be set in an FOC S1SPKI End Entity Certificate or FOC S1SPKI CA Certificate other than in accordance with this Part 6.1.7.

6.2 Private Key Protection and Cryptographic Module Engineering Controls

6.2.1 Cryptographic module standards and controls

(A) The FOC S1SP shall ensure that the FOC S1SPKI CPS incorporates detailed provision in relation to the cryptographic module, standards, and controls to be established and operated for the purposes of the exercise of its functions as the FOC S1SPKI CA. Which should include, but not be limited to:

(i) ensuring that all FOC S1SPKI CA Private Keys shall be:

(a) protected to a high standard of assurance by physical and logical security controls; and

(b) stored in and operated from within a Cryptographic Module which is compliant with FIPS 140-2 Level 3 (or any equivalent to that Federal Information Processing Standard which updates or replaces it from time to time).

(ii) ensuring that all FOC S1SPKI CA Private Keys shall, where they affect the outcome of any Certificates Issued by it, be protected by, stored in and operated from within a Cryptographic Module which is compliant with FIPS 140-2 Level 3 (or any equivalent to that Federal Information Processing Standard which updates or replaces it from time to time).

(iii) ensuring that no FOC S1SPKI CA Private Key shall be made available in either complete or unencrypted form except in a Cryptographic Module which is compliant with FIPS 140-2 Level 3 (or any equivalent to that Federal Information Processing Standard which updates or replaces it from time to time).

(iv) ensuring that any Cryptographic Module which is used for any purpose related to Certificate life-cycle management shall:

(a) operate so as to block access to itself following a number of failed consecutive attempts to access it using Activation Data, where that number shall be set out in the Organisation CPS; and

(b) require to be unblocked by an authorised Privileged User who has been Authenticated as such following a process which shall be set out in the Organisation CPS.

6.2.2 Private Key (n out of m) multi-person control

(A) See Part 6.1.1 of this Policy and the FOC S1SPKI CPS for further details.

6.2.3 Private Key escrow

(A) This Policy does not support Key Escrow.

(B) The FOC S1SPKI CA shall not provide any Key Escrow service.

6.2.4 Private Key backup

(A) The FOC S1SPKI CA may Back-Up FOC S1SPKI CA Private Keys insofar as:

(i) each Private Key is protected to a standard which is at least equivalent to that required in relation to the principal Private Key in accordance with this Policy; and

(ii) where more than one Private Key is Backed-Up within a single security environment, each of the Private Keys which is Backed-Up within that environment must be protected to a standard which is at least equivalent to that required in relation to an FOC S1SPKI CA Private Key in accordance with this Policy.

(B) Participants providing trust services may backup and archive Private Keys, including CA-keys.

6.2.5 Private Key archival

No stipulation.

6.2.6 Private Key transfer into or from a cryptographic module

(A) The FOC S1SP shall ensure that the FOC S1SPKI CPS incorporates detailed provision in relation to the FOC S1SPCA Private Key transfer into or from a cryptographic module for the following purposes only:

(i) Back-Up; or

(ii) establishing an appropriate degree of resilience in relation to the provision of the SMKI Services; and

(iii) where such transfers are in accordance with a level of protection which is compliant with FIPS 140-2 Level 3 (or any equivalent to that Federal Information Processing Standard which updates or replaces it from time to time).

6.2.7 Private Key storage on cryptographic module

(A) See Part 6.2.1 of this Policy.

6.2.8 Method of activating Private Key

(A) The FOC S1SP shall ensure that the FOC S1SPKI CPS incorporates detailed provision in relation to the method of activating a Private Key, whereby:

(i) The FOC S1SPKI CA shall ensure that the Cryptographic Module in which any FOC S1SPKI CA Private Key is stored may be accessed only by a Privileged User who has been Authenticated following an Authentication process which:

(a) has an appropriate level of strength to ensure the protection of the Private Key; and

(b) involves the use of Activation Data.

6.2.9 Method of deactivating Private Key

(A) The FOC S1SP shall ensure that any FOC S1SPKI CA Private Key shall be capable of being de-activated by means of the FOC S1SPKI CA Systems, at least by:

(i) the actions of:

(a) turning off the power;

(b) logging off;

(c) carrying out a system reset; or

(d) a period of inactivity of a length which shall be set out in the FOC S1SPKI CPS.

6.2.10 Method of destroying Private Key

(A) The FOC S1SP shall ensure that the FOC S1SPKI CPS incorporates provisions for the exercise of strict controls in relation to the destruction of FOC S1SPKI CA Keys.

(B) The FOC S1SP shall ensure that no FOC SS1SPKI CA Key (whether in active use, existing as a copy for the purposes of resilience, or Backed-Up) is destroyed except in accordance with a positive decision by the DCC or the FOC S1SP ITSC instructing the FOC S1SPKI CA to destroy it.

6.2.11 Cryptographic Module Rating

(A) See Part 6.2.1 of this Policy.

6.3 Other aspects of key pair management

6.3.1 Public key archival

(A) The FOC S1SPKI CA shall ensure that it archives Public Keys in accordance with the requirements of Part 5.5 of this Policy.

6.3.2 Certificate operational periods and key pair usage periods

(A) The FOC S1SPKI CA shall ensure that the Validity Period of each Certificate Issued by it shall be as follows:

Certificate	Validity (Years)
Operator Root CA Certificate	25 years
Intermediate Operator CA Certificate	20 years
Intermediate Enterprise CA Certificate	20 years
End Entity Operator Device Certificate	5 years
End Entity Push Certificate	5 years
End Entity Server Certificate	5 years
Application Service Root CA Certificate	25 years
Intermediate Application Service PKI CA Certificate	20 years
End Entity PKI Role CA Certificate	5 years
End Entity PKI Role RA Certificate	5 years

6.4 Activation Data

6.4.1 Activation Data generation and installation

(A) The FOC S1SPKI CA shall ensure that any secure container within which a FOC S1SPKI CA Private Key is held has Activation Data that are unique and unpredictable.

(B) The FOC S1SPKI CA shall ensure that:

(C) these Activation Data, in conjunction with any other access control, shall be of an appropriate level of strength for the purposes of protecting the FOC S1SPKI CA Private Keys; and

(D) where the Activation Data comprise any PINs, passwords or passphrases, the FOC S1SPKI CA shall have the ability to change these at any time.

6.4.2 Activation data protection

(A) The FOC S1SP shall ensure that the FOC S1SPKI CPS incorporates provision for the use of such cryptographic protections and access controls as are appropriate to protect against the unauthorised use of Activation Data.

6.4.3 Other Aspects of Activation Data/

[Not applicable in this Policy]

6.5 Computer Security Controls

6.5.1 Specific Computer Security Technical Requirements

(A) The FOC S1SP shall ensure that the FOC S1SPKI CPS incorporates provisions in relation to the identification and implementation, following the conclusion of any threat assessment, of security measures which make provision for at least the following:

(i) the establishment of access controls in relation to the activities of the FOC S1SPKI CA;
(ii) the appropriate allocation of responsibilities to Privileged Users;
(iii) the identification and Authentication of organisations, individuals and Systems involved in FOC S1SPKI CA activities;
(iv) the use of cryptography for communication and the protection of Data stored on the FOC S1SPKI CA Systems;
(v) the audit of security related events; and
(vi) the use of recovery mechanisms for FOC S1SPKI CA Keys.

6.5.2 Computer security rating

(A) The FOC S1SP shall ensure that the Organisation CPS incorporates provisions relating to the appropriate security rating of the FOC S1SPKI CA Systems.

(B) The FOC S1SP may, where not specifically required to under this Policy, use certain system components that do not possess a formal computer security rating provided that all requirements of this Policy are satisfied.

6.6 Life cycle technical controls

6.6.1 System development controls

(A) The FOC S1SPshall ensure that any software which is developed for the purpose of establishing a functionality of the FOC S1SPKI CA Systems shall:
(i) take place in a controlled environment that is sufficient to protect against the insertion into the software of malicious code;
(ii) be undertaken by a developer which has a quality system that is:
(a) compliant with recognised international standards (such as ISO 9001:2000 or an equivalent standard); and

(B) where so required, be available for inspection and approval by the DCC or the FOC S1SP ITSC and has been so inspected and approved where the case may be.

6.6.2 Security management controls

(A) The FOC S1SP shall ensure that the FOC S1SPKI CPS incorporates provisions which are designed to ensure that the FOC S1SPKI CA Systems satisfy the requirements of Section G2 (System Security: Obligations on the DCC) and Section G5 (Information Security: Obligations on the DCC and Users) of the Code.

(B) As a minimum the scope of the FOC S1SPKI must achieve certification with following information security standard:
(i) ISO/IEC 27001:2013 (Information Technology – Security Techniques – Information Security Management Systems); or
(ii) any equivalent to that standard which updates or replaces it from time to time.

(C) The FOC S1SP shall also ensure that the FOC S1SPKI shall be independently assessed against an assurance scheme:
(i) which is recognised as an accreditation scheme for the purposes of Article 3(2) of Directive 1999/93/EC on a Community framework for electronic signatures;
(ii) which is based on ISO 27001; and
(iii) the provider of which:
(a) is used by the United Kingdom Government to provide assurance in relation to electronic trust services; and
(b) requires all its scheme assessors to be UKAS certified.

6.6.3 Life cycle security controls

(A) See Part 6.6.2 of this Policy.

6.7 Network security controls

6.7.1 Use of Offline Operator Root CA

(A) The FOC S1SP shall ensure that its functions as the FOC S1SPKI CA are carried out on a part of the FOC S1SPKI CA Systems that is neither directly nor indirectly connected to any System which is not a part of the FOC S1SPKI CA Systems.

(B) The Operator Root CA, when not operational, should be kept offline with no direct or indirect network access.

(C) The FOC S1SP shall ensure that the FOC S1SPKI CPS incorporates provisions which are designed to ensure the requirements of paragraphs (A) and (B) above.

6.7.2 Protection Against Attack

(A) The FOC S1SP shall ensure that the FOC S1SPKI CPS incorporates provisions in relation to:

- (i) using its best endeavours to ensure that the FOC S1SPKI Systems are not Compromised, and in particular for this purpose that they are designed and operated so as to detect and prevent:
- (ii) any Denial of Service Event; and
- (iii) any unauthorised attempt to connect to them.

(B) using all reasonable to steps to ensure that the FOC S1SPKI CA Systems cause or permit to be open at any time only those network ports, and allow only those protocols, which are required at that time for the effective operation of those Systems, and block all network ports and protocols which are not so required.

6.7.3 Separation of FOC S1SP Intermediate CAs

(A) The FOC S1SP shall ensure that, where its functions as the FOC S1SP Intermediate CA are carried out on a part of the FOC S1SPKI CA Systems that is connected to an external network, they are carried out on a System that is Separated from all other FOC S1SPKI CA Systems.

6.7.4 Health Check of FOC SS1SPCA Systems

(A) The FOC S1SP shall ensure that, in relation to the FOC S1SPKI CA Systems, a vulnerability assessment in accordance with Section G2.13 of the Code (Management of Vulnerabilities) is carried out with such frequency as may be specified from time to time by the Independent S1SPKM Assurance Service Provider.

6.8 Time-Stamping

6.8.1 Use of Time-Stamping

(A) The FOC S1SP shall ensure that Timestamping takes place in relation to all Certificates and all other FOC S1SPKI CA activities which require an accurate record of time.

(B) The FOC S1SP shall ensure that the FOC S1SPKI CA incorporates provisions in relation to the time source and mechanisms used by any Time-Stamping Authority which carries out Time-Stamping on behalf of the FOC S1SPKI CA.

7 CERTIFICATE, CRL PROFILES

7.1 Certificate profile

(A) The FOC S1SPCA shall only Issue Certificates in accordance with the Certificate Profiles in Annex B of this Policy.

7.1.1 Version number(s)

(A) See Annex B of this Policy.

7.1.2 Certificate extensions

(A) See Annex B of this Policy.

(B) The FOC S1SPKI CA shall process the extensions identified in sections 4.2.1 and 4.2.2 of the IETF RFC 5280 Certificate Profile Specification. The following are common Certificate extensions:

I. The Basic Constraints extension is set to TRUE for CA-Certificates only; its use is critical specifying that it is a CA-Certificate. Subscriber End Entity Certificates have the value set to FALSE.

7.1.3 Algorithm object identifiers

(A) See Annex B of this Policy.

7.1.4 Name forms

(A) See Annex B of this Policy.

7.1.5 Name constraints

(A) See Annex B of this Policy.

7.1.6 Certificate policy object identifier

(A) See Part 1.2 of this Policy.

7.1.7 Usage of Policy Constraints extension

(A) See Annex B of this Policy.

7.1.8 Policy qualifiers syntax and semantics

(A) See Annex B of this Policy.

7.1.9 Processing semantics for the critical Certificate Policies extension

(A) See Annex B of this Policy.

7.2 CRL profile

7.2.1 Version number(s)

(A) The FOC S1SPKI CA shall ensure that the FOC S1SP ARL and FOC S1SP CRL conform with X.509 v3 and IETF RFC 5280.

7.2.2 CRL and CRL entry extensions

(A) [Not applicable in this Policy].

7.3 OCSP profile

7.3.1 Version number(s)

(A) An OCSP service is not applicable in this Policy.

7.3.2 OCSP extensions

(A) [Not applicable in this Policy].

8 COMPLIANCE AUDIT AND OTHER ASSESSMENTS

8.1 Frequency or circumstances of assessment

(A) Provision in relation to this is made in Appendix AO of the Code (S1SPKM Compliance Policy).

8.2 Identity/qualifications of assessor

(A) Provision in relation to this is made in Appendix AO of the Code (S1SPKM Compliance Policy).

8.3 Assessor's relationship to assessed entity

(A) Provision in relation to this is made in Appendix AO of the Code (S1SPKM Compliance Policy).

8.4 Topics covered by assessment

(A) Provision in relation to this is made in Appendix AO of the Code (S1SPKM Compliance Policy).

8.5 Actions taken as a result of deficiency

(A) Provision in relation to this is made in Appendix AO of the Code (S1SPKM Compliance Policy).

8.6 Communication of results

(A) Provision in relation to this is made in Appendix AO of the Code (S1SPKM Compliance Policy).

9 OTHER BUSINESS AND LEGAL MATTERS

(A) This document forms part of the Smart Energy Code and the DCC is required to ensure that the FOCS1SPKI is implemented and operated in accordance with this Policy and the associated FOC S1SPKI CPS.

9.1 Fees

9.1.1 Certificate issuance or renewal fees

See the statement at the beginning of this Part.

9.1.2 Certificate access fees

See the statement at the beginning of this Part.

9.1.3 Revocation or status information access fees

See the statement at the beginning of this Part.

9.1.4 Fees for other services

See the statement at the beginning of this Part.

9.1.5 Refund policy

See the statement at the beginning of this Part.

9.2 Financial responsibility

9.2.1 Insurance coverage

See the statement at the beginning of this Part.

9.2.2 Other assets

See the statement at the beginning of this Part.

9.2.3 Insurance or warranty coverage for end-entities

See the statement at the beginning of this Part.

9.3 Confidentiality of business information

9.3.1 Scope of confidential information

See the statement at the beginning of this Part.

9.3.2 Information not within the scope of confidential information

See the statement at the beginning of this Part.

9.3.3 Responsibility to protect confidential information

See the statement at the beginning of this Part.

9.4 Privacy of personal information

See the statement at the beginning of this Part.

9.4.1 Privacy plan

See the statement at the beginning of this Part.

9.4.2 Information treated as private

See the statement at the beginning of this Part.

9.4.3 Information not deemed private

See the statement at the beginning of this Part.

9.4.4 Responsibility to protect private information

See the statement at the beginning of this Part.

9.4.5 Notice and consent to use private information

See the statement at the beginning of this Part.

9.4.6 Disclosure pursuant to judicial or administrative process

See the statement at the beginning of this Part.

9.4.7 Other information disclosure circumstances

See the statement at the beginning of this Part.

9.5 Intellectual property rights

See the statement at the beginning of this Part.

9.6 Representations and warranties

See the statement at the beginning of this Part.

9.7 Disclaimers of warranties

See the statement at the beginning of this Part.

9.8 Limitations of liability

See the statement at the beginning of this Part.

9.9 Indemnities

See the statement at the beginning of this Part.

9.10 Term and termination

9.10.1 Term

See the statement at the beginning of this Part.

9.10.2 Termination

See the statement at the beginning of this Part.

9.10.3 Effect of termination and survival

See the statement at the beginning of this Part.

9.11 Individual notices and communications with participants

9.11.1 Subscribers

See the statement at the beginning of this Part.

9.11.2 Issuing Authority

See the statement at the beginning of this Part.

9.11.3 Notification

See the statement at the beginning of this Part.

9.12 Amendments

9.12.1 Procedure for amendment

See the statement at the beginning of this Part.

9.12.2 Notification mechanism and period

See the statement at the beginning of this Part.

9.12.3 Circumstances under which OID must be changed

See the statement at the beginning of this Part.

9.13 Dispute resolution provisions

See the statement at the beginning of this Part.

9.14 Governing law

See the statement at the beginning of this Part.

9.15 Compliance with applicable law

See the statement at the beginning of this Part.

9.16 Miscellaneous provisions

9.16.1 Entire agreement

See the statement at the beginning of this Part.

9.16.2 Assignment

See the statement at the beginning of this Part.

9.16.3 Severability

See the statement at the beginning of this Part.

9.16.4 Enforcement (attorneys' fees and waiver of rights)

See the statement at the beginning of this Part.

9.16.5 Force Majeure

See the statement at the beginning of this Part.

9.17 Other provisions

9.17.1 Certificate Policy Content

See the statement at the beginning of this Part.

9.17.2 Third party rights

See the statement at the beginning of this Part.

Glossary

10 Annex A: Definitions and Interpretation

Definitions	Interpretations
Activation	means the process of making the FOC S1SP HES and Operator Private Keys stored available for use.
Activation Data	means any private Data (such as a password or the Data on a smartcard) which are used to access a Security Container.
Application Service End Entity Certificate	means either an End Entity PKI Role CA Certificate or an End Entity PKI Role RA Certificate issued by an Intermediate Application Service PKI CA as set out in Annex B of this Policy.
Application Service CA	means the FOC S1SP exercising the function of the Application Service Root CA to Issue Certificates to the Intermediate Application Service PKI CA and the Intermediate Application Service PKI CA and storing and managing Private Keys associated with those functions.
Application Service CA Certificate	means either an Application Service Root CA Certificate or an Intermediate Application Service CA Certificate.
Application Service PKI	means one of the three public key infrastructures that support the operation of each of the FOC S1SP Operator Root CA, the Intermediate Operator CA and the Intermediate Enterprise CA.
Application Service Registration Authority (Application Service RA)	Means the Application Service CA exercising the function of receiving and processing Certificate Signing Requests and Certificate Revocation Requests made in accordance with Annex E: FOC S1SPKI RAPP of this Policy.
Application Service Root Certification Authority (Application Service Root CA)	means the FOC S1SP exercising the functions of each or all of three Application Service Root CAs to Issue Intermediate Application Service PKI CA Certificates to each or all of the three Intermediate Application Service PKI CAs and storing and managing Private Keys associated with that function.
Application Service Root CA Certificate	means one of the self-signed Certificate issued by the Application Service Root CA that meets the requirements of the Application Service Root CA Certificate profile set out in Annex B and which is issued in accordance with this Policy.
Archive	means the archive of Data created in accordance with Part 5.5.1 of this Policy (and “Archives” and “Archived” shall be interpreted accordingly).
Audit Log	means the audit log created in accordance with Part 5.4.1 of this Policy and the FOC S1SPKI CPS.
Authentication	means the process of establishing that an individual, Certificate, System, SMETS1 Device or Organisation is what he or it claims to be (and “Authenticate” shall be interpreted accordingly).
Authorised Subscriber	means one of the entities described as such in Annex E of this Policy.
Back-Up	means, in relation to Data which is held on any FOC S1SP HES System, the storage of a copy of that Data for the purpose of ensuring that the copy may be used (if required) to restore or replace the original Data; and “Backed-Up” is to be interpreted accordingly.
Certificate	means any public key certificate Issued under this Certificate Policy by the FOC S1SPCA or the Application Service CA, the certificate being an electronic document issued by a FOC S1SPCA that is used to prove the

	ownership of a Public Key. Valid Certificates under this Policy are: - FOC S1SPCA Certificates; - FOC S1SP End Entity Certificates; - Application Service CA Certificates; - Application Service End Entity Certificates.
Certification Authority	means the FOC S1SPCA and/or the Application Service CA as the context requires.
Certificate Policy (known as the 'Policy' in this document)	is a document which aims to state what are the different entities of a Public Key Infrastructure (PKI), their roles and their duties.
Certificate Profile	means a table bearing that title in Annex B and specifying certain parameters to be contained within a Certificate.
Certificate Revocation List Distribution Point (CDP)	means a shared location on the network that is used to store the CRLs
Certificate Re-Key	means a change to the Public Key contained within a Certificate bearing a particular serial number which results in a new Certificate being issued.
Certificate Revocation Request (CRR)	means a request for the revocation of a Certificate made to the FOC S1SPCA, submitted in accordance with the FOC S1SPKI RAPP and this Policy.
Certificate Signing Request (CSR)	means a request for a Certificate submitted by an Authorised Subscriber in accordance with the FOC S1SPKI RAPP as set out in Annex E of this Policy.
Certificate Status	Provides details of the validity of Certificates and includes Revocation information.
Cryptographic Module	Means a Security Container.
Cryptographic Processing	means the generation, storage or use of any Secret Key Material
Data	means any information, data, knowledge, figures, methodologies, minutes, reports, forecasts, images or sounds (together with any database made up of any of these) embodied in any medium (whether tangible or electronic).
Eligible Subscriber	means one of the entities described as such (and in relation to the relevant Certificate types) in Annex E of this Policy:
End Entity Operator Device Certificate	A Certificate issued by the Operator CA that meets the requirements of the End Entity Operator Device Certificate profile set out in Annex B and which is issued in accordance with this Policy.
End Entity PKI Role CA Certificate	means one of the Certificates issued by an Intermediate Application Service PKI CA that meets the requirements of the End Entity PKI Role CA Certificate profile set out in Annex B and which is issued in accordance with this Policy.
End Entity PKI Role RA Certificate	means one of the Certificates issued by an Intermediate Application Service PKI CA that meets the requirements of the End Entity PKI Role RA Certificate profile set out in Annex B and which is issued in accordance with this Policy.
End Entity Push Certificate	A Certificate issued by the Enterprise CA that meets the requirements of the End Entity Push Certificate profile set out in Annex B and which is issued in accordance with this Policy.
End Entity Server Certificate	A Certificate issued by the Enterprise CA that meets the requirements of the End Entity Server Certificate profile set out in Annex B and which is issued in accordance with this Policy.

FOC S1SP	Means any one of the following DCC Service Providers responsible for the delivery and operation of the FOC S1SPKI service: • TRILLIANT NETWORKS OPERATIONS (UK) LTD] (registered in England and Wales under number 011321639 whose registered office is at Morgan House, Madeira Walk, Windsor, Berkshire SL4 1EP acting in its capacity as a DCC Service Provider. • CAP GEMINI UK PLC (registered in England and Wales under number 00943935 whose registered office is at No. 1 Forge End, Woking, Surrey, GU21 6DB acting in its capacity as a DCC Service Provider. • (DXC) ENTSERV UK LIMITED (registered in England and Wales under number 00053419 whose registered office is at Royal Pavilion, Wellesley road, Aldershot, GU11 1PZ, acting in its capacity as a DCC Service Provider. Where they are acting in the capacity of, and exercising the functions of one or more of: (a) FOC S1SPCA; (b) the FOC S1SPKI Registration Authority; (c) and any other aspects of the wider FOC S1SPKI Systems.
FOC S1SP Authority Revocation List (FOC S1SP ARL)	means a list, produced by the FOC S1SPCA, of all FOC S1SPCA Certificates that have been revoked in accordance with this Policy.
FOC S1SP CA Certificates	Means either an Operator Root CA Certificate, an Intermediate Enterprise CA Certificate or an Intermediate Operator CA Certificate as set out in Annex B of this Policy.

FOC S1SP Certification Authority (or FOC S1SPCA)	means the FOC S1SP, acting in the capacity and exercising the functions of one or more of the:
	(a) FOC S1SP Operator Root CA;
	(b) Intermediate Operator CA;
	(c) Intermediate Enterprise CA;
	(d) FOC S1SPCA Systems; and
	(e) FOC S1SP PKI Registration Authority.

FOC S1SP Certificate Revocation List (FOC S1SPKI CRL)	means a list, produced by the FOC S1SPKI Intermediate CA, of all FOC S1SP End Entity Certificates that have been revoked in accordance with this Certification Policy.
FOC S1SP End Entity Certificates	means either an End Entity Server Certificate, an End Entity Push Certificate, or an End Entity Operator Device Certificate issued by a FOC S1SP CA as set out in Annex B of this Policy.
FOC S1SP Head End System	means the head end system which is used by the FOC S1SP to communicate with SMETS1 CHs.
FOC S1SP Intermediate Certification Authority (FOC S1SP Intermediate CA)	means the FOC S1SP exercising the function of the FOC S1SP Intermediate Enterprise CA and the Intermediate Operator CA to Issue FOC S1SP End Entity Certificates in accordance with Annex B of this Policy.
FOC S1SP Intermediate Certification Authority Certificate (FOC S1SP Intermediate CA Certificate)	Means either an Intermediate Enterprise CA Certificate or an Intermediate Operator CA Certificate as set out in Annex B of this Policy and Issued by the FOC S1SP Root CA in accordance with this Policy.
FOC S1SP Intermediate Certification Authority Private Key (FOC S1SP Intermediate CA Private Key)	Means either: • The Intermediate Operator CA Private Key; or • The Intermediate Enterprise CA Private Key.

FOC S1SP Intermediate Certification Authority Service Provider (FOC S1SP Intermediate CA SP)	Means (DXC) ENTSERV UK LIMITED (registered in England and Wales under number 00053419 whose registered office is at Royal Pavilion, Wellesley road, Aldershot, GU11 1PZ, acting in its capacity as a DCC Service Provider.
FOC S1SP Operator Root Certification Authority (CA)	means the FOC S1SP exercising the function of the FOC S1SP Operator Root CA to Issue Certificates to the FOC S1SP Operator Root CA and the FOC S1SP Intermediate CA and storing and managing Private Keys associated with those functions.
FOC S1SP Operator Root Certification Authority Service Provider (FOC S1SP Operator Root CA SP)	means CAP GEMINI UK PLC (registered in England and Wales under number 00943935 whose registered office is at No. 1 Forge End, Woking, Surrey, GU21 6DB acting in its capacity as a DCC Service Provider.
FOC S1SPKI	means the S1SPKIs operated by the FOC S1SP including the FOC S1SP Head End Systems, FOC S1SPCA Systems, personnel, policy and procedures and any public key infrastructure established (or to be established) by FOC S1SP for the purpose, among other things, of providing secure communications between FOC S1SP, the DCC and SMETS1 Devices. It also includes the Application Service PKIs.
FOC S1SPKI CA	Means the FOC S1SPCA and the Application Service CA.
FOC S1SPKI CA Certificate	Means any FOC S1SPCA Certificate and any Application Service CA Certificate.
FOC S1SPKI CA Private Key	Any Private Key associated with a Public Key contained with any FOC S1SPCA Certificate or any Application Service CA Certificate.
FOC S1SPKI CA Key Pair	A Public Key that is (or is to be) contained within any FOC S1SPCA Certificate or any Application Service CA Certificate and the associated Private Key.
FOC S1SPKI CPS	means the Certification Practice Statement describing how this PKI is operated and maintained and corresponds to this Policy
FOC S1SPKI End Entity Certificate	Means any FOC S1SPKI End Entity Certificate or any Application Service End Entity Certificate.
FOC S1SPKI Personnel	means those persons who are engaged by the FOC S1SP under this Policy, in so far as such persons carry out, or are authorised to carry out, any function of such FOC S1SPKI System or FOC S1SPCA or Application service CA but not Registration Authority functions (see FOC S1SPKI RA Personnel).
FOC S1SPKI RAPP	is set out in the SEC document set and is the Registration Authority Policy and Procedures (RAPP) for this policy document
FOC S1SPKI Registration Authority (RA)	Means the FOC S1SPKI CA exercising the function of receiving and processing Certificate Signing Requests and Certificate Revocation Requests made in accordance with Annex E: FOC S1SPKI RAPP of this Policy.
FOC S1SPKI Registration Authority Manager	means either a director of the FOC S1SP or any other person who may be identified as such in accordance with Annex E: FOC S1SPKI RAPP of this Policy.
FOC S1SPKI Registration Authority Personnel (FOC S1SPKI RA Personnel)	means those persons who are engaged by the FOC S1SP, in so far as such persons carry out, or are authorised to carry out, any function of the FOC S1SPKI Registration Authority
FOC S1SPKI Repository	For the purposes of the FOC S1SPKI, the “FOC S1SPKI Repository” means a number of Systems for storing and (subject to

	the provisions of this Policy) making available copies of Certificates Issued pursuant to the Policy.
Hardware Security Module (HSM)	means a security module is a physical computing device that safeguards and manages digital keys, performs encryption and decryption functions for digital signatures, strong authentication and other cryptographic functions
Intermediate Application Service PKI CA Certificate	means one of the Certificates issued by the Application Service Root CA that meets the requirements of the Intermediate Application Service PKI CA Certificate profile set out in Annex B and which is issued in accordance with this Policy.
Intermediate Enterprise Certification Authority (Intermediate Enterprise CA)	means the FOC S1SP exercising the function of the Intermediate Enterprise CA to Issue End Entity Push Certificates, End Entity Server Certificates, and of storing and managing the Private Keys associated with that function.
Intermediate Enterprise Certification Authority Certificate (Intermediate Enterprise CA Certificate)	means a Certificate in the form set out in the Intermediate Enterprise CA Certificate Profile in accordance with Annex B and Issued by the FOC S1SP Root CA to the Intermediate Enterprise CA in accordance with this Policy.
Intermediate Enterprise Certification Authority Private Key (Intermediate Enterprise CA Private Key)	means a Private Key that forms a Key Pair with a Public Key held within Intermediate Enterprise CA Certificate.
Intermediate Operator CA Certificate (Intermediate Operator CA Certificate)	means a Certificate in the form set out in the Intermediate Operator CA Certificate Profile in accordance with Annex B and Issued by the FOC S1SP Root CA to the Intermediate Operator CA in accordance with this Policy.
Intermediate Operator Certification Authority (Intermediate Operator CA)	means the FOC S1SP exercising the function of the Intermediate Operator CA to Issue End Entity Operator Device Certificates and of storing and managing the Private Keys associated with that function.
Intermediate Operator Certification Authority Private Key (Intermediate Operator CA Private Key)	means a Private Key that forms a Key Pair with a Public Key held within Intermediate Operator CA Certificate.
Intermediate Application Service PKI Certification Authority (Intermediate Application Service PKI CA)	means the FOC S1SP exercising the functions of each or all of the three Intermediate Application Service PKI CAs to Issue End Entity PKI Role CA Certificates and End Entity PKI Role RA Certificates and storing and managing Private Keys associated with that Function.
Operator Root CA Certificate	means one of the self-signed Certificates issued by the FOC S1SP Operator Root CA that meets the requirements of the Operator Root CA Certificate profile set out in Annex B and that has been issued in accordance with Policy.
Policy	means this FOC S1SP Certificate Policy.
Private Key	means the private part of an asymmetric Key Pair used for the purposes of public key cryptography and which is associated with a Public Key that is contained within any Certificate that is Issued (or to be Issued) in accordance with this Policy.
Private Key Material	in relation to a Private Key, means that Private Key and the input parameters necessary to establish, use and maintain it.
Privileged User	means a FOC S1SPKI Personnel or FOC S1SPKI RA Personnel who is authorised to carry out activities which involve access to resources, or Data held, on the FOC S1SPCA System and which are capable of being a means by which the FOC S1SPCA System (or are capable of being) being compromised to a material extent

Public Key	means the public part of an asymmetric Key Pair used for the purposes of public key cryptography.
Public Key Infrastructure	is a set of roles, policies, hardware, software and procedures needed to create, manage, distribute, use, store and revoke digital Certificates and manage public-key encryption
Relying Party	means any System, Device, organisation or individual that relies on a Certificate that has been Issued under this Policy.
S1SP	means SMETS1 Service Provider
S1SPKI	means any public key infrastructure established (or to be established) for the purpose, among other things, of providing secure communications between the DCC and SMETS1 Devices.
S1SPKI CA Systems	means the FOC S1SPCA Systems and the Application Service CA Systems.
Secret Key Material	means any Private Key, Shared Secret, Symmetric Key or other functionally equivalent cryptographic material (and any associated input parameter) that is generated and maintained by the FOC S1SP CA
Security Container	means a set of hardware, software and/or firmware that is designed for : a) the secure storage of Secret Key Material; and b) the implementation of Cryptographic Processing without revealing Secret Key Material.
Security Related Functionality	means the functionality of the FOC S1SP HES Systems which is designed to detect, prevent or mitigate the adverse effect of any security compromise of that System.
Security Sub-Committee or SSC	means the Security Sub-Committee under the Smart Energy Code
Smart Energy Code	means the code of that name maintained pursuant to the smart meter communication licences granted under the UK Gas Act 1986 and the UK Electricity Act 1989
SMETS1	means the Smart Metering Equipment Technical Specifications 1
Subject	the Subject of any Certificate is the entity identified in the subject field of that Certificate
Subscriber	the FOC S1SPKI Systems or a person engaged by the S1SPKI CA (acting on behalf of the S1SPKI CA) to which a Certificate has been Issued in accordance with the requirements of this Policy.
System	means a system for generating, sending, receiving, storing (including for the purposes of Back-Up), manipulating or otherwise processing electronic communications, including all hardware, software, firmware, databases and Data associated with issuing Certificates in accordance with this Policy.
Task Manager	is a function in the Trilliant software which instructs an API to perform specific tasks such as certificate administration services.
Timestamping	means the act that takes place when a Time-Stamping Authority, in relation to a Certificate, stamps a particular datum with an accurate indicator of the time (in hours, minutes and seconds) at which the activity of stamping takes place.
Timestamping Authority	A trusted timestamp is a timestamp issued by a Trusted Third Party (TTP) acting as a Time Stamping Authority

	(TSA). It is used to prove the existence of certain data before a certain point without the possibility that the owner can backdate the timestamps.
Trust Store	or Repository holding the Certificates for each trusted CA
Validity Period	means, in respect of a Certificate, the period of time for which that Certificate is intended to be valid.

11 Annex B: FOC S1SP CA and End Entity Certificate Profiles

11.1 Certificate Structure and Contents

(A) This Annex lays out requirements as to structure and content with which FOC S1SPCA Certificates and FOC S1SP End Entity Certificates shall comply. All terms in this Annex shall, where not defined in this Policy, or the GB Companion Specification (GBCS), have the meanings in IETF RFC 5759 or IETF RFC5280.

11.2 Common requirements applicable to FOC S1SPCA Certificates and FOC S1SP End Entity Certificates

(A) All Certificates shall be compliant with IETF RFC 5759 and so with IETF RFC5280.The FOC S1SPCA shall only issue X.509 v3 certificates as defined in IETF RFC 5280 and IETF RFC 6818.

Public Key and algorithm	Issued Certificates	Internal TLS Certificates
Signature Algorithm	OID 1.2.840.10045.4.3.2 [ecdsa-with-SHA256]	OID 1.2.840.10045.4.3.2 [ecdsa-with-SHA256]
Subject Public Key	OID 1.2.840.10045.3.1.7 [ECDSA secp256r1]	OID 1.3.132.0.34 [ECDSA secp384r1]

Operator Root Certificate

Number of Keys: One per environment

Data Field	Value		
Version	v3		
Serial Number	[Automatic no. according to Verisign standard]		
Signature Algorithm	ecdsa-with-SHA256 (OID 1.2.840.10045.4.3.2)		
Issuer	Attribute	Value	Encoding
	CN	Operator Root	Printable String
	O	[Environment Specific]	Printable String
	C	GB	Printable String
Validity	[Per DCC validity period specification]		
Subject	Attribute	Value	Encoding
	CN	Operator Root	Printable String
	O	[Environment Specific]	Printable String
	C	GB	Printable String
Subject Public Key	ECDSA secp256r1 (OID 1.2.840.10045.3.1.7) according SECG Standard		
Extension	Crit.	Value	
`basicConstraints`	yes	cA: TRUE	
`keyUsage`	yes	`keyCertSign, cRLSign`	

Intermediate Operator CA Certificate

Number of keys: One per environment

Data Field	Value		
Version	v3		
Serial Number	[Automatic no. according to Verisign standard]		
Signature Algorithm	ecdsa-with-SHA256 (OID 1.2.840.10045.4.3.2)		
Issuer	Attribute	Value	Encoding
	CN	Operator Root	Printable String
	O	[Environment Specific]	Printable String
	C	GB	Printable String
Validity	[Per DCC validity period specification]		
Subject	Attribute	Value	Encoding
	CN	Operator	Printable String
	O	[Environment Specific]	Printable String
	C	GB	Printable String
Subject Public Key	ECDSA secp256r1 (OID 1.2.840.10045.3.1.7) according SECG Standard		
Extension	Crit.	Value	
`basicConstraints`	yes	cA: TRUE	
`keyUsage`	yes	`keyCertSign, cRLSign`	

Intermediate Enterprise CA Certificate

Number of keys: One per environment

Data Field	Value		
Version	v3		
Serial Number	[Automatic no. according to Verisign standard]		
Signature Algorithm	ecdsa-with-SHA256 (OID 1.2.840.10045.4.3.2)		
Issuer	Attribute	Value	Encoding
	CN	Operator Root	Printable String
	O	[Environment Specific]	Printable String
	C	GB	Printable String
Validity	[Per DCC validity period specification]		
Subject	Attribute	Value	Encoding
	CN	Enterprise	Printable String
	O	[Environment Specific]	Printable String
	C	GB	Printable String
Subject Public Key	ECDSA secp256r1 (OID 1.2.840.10045.3.1.7) according SECG Standard		
Extension	Crit.	Value	
`basicConstraints`	yes	cA: TRUE	
`keyUsage`	yes	`keyCertSign, cRLSign`	

End Entity Operator Device Certificate

Number of keys: One per device

Data Field	Value		
Version	v3		
Serial Number	[Automatic no. according to Verisign standard]		
Signature Algorithm	ecdsa-with-SHA256 (OID 1.2.840.10045.4.3.2)		
Issuer	Attribute	Value	Encoding
	CN	Operator	Printable String
	O	[Environment Specific]	Printable String
	C	GB	Printable String
Validity	[Per DCC validity period specification]		
Subject	Attribute	Value	Encoding
	CN	[Dynamic Per Device]	Printable String
	OU	[Environment Specific]	Printable String
	O	[Environment Specific]	Printable String
	C	GB	Printable String
Subject Public Key	ECDSA secp256r1 (OID 1.2.840.10045.3.1.7) according SECG Standard		
Extension	**Critical**	**Value**	
`basicConstraints`	yes	cA: FALSE	
`keyUsage`	yes	`digitalSignature; keyAgreement`	
`extKeyUsage`	no	TLS Web Server Authentication	

End Entity Push Certificate

Number of keys: One per environment (HES instance)

Data Field	Value		
Version	v3		
Serial Number	[Automatic no. according to Verisign standard]		
Signature Algorithm	ecdsa-with-SHA256 (OID 1.2.840.10045.4.3.2)		
Issuer	Attribute	Value	Encoding
	CN	Enterprise	Printable String
	O	[Environment Specific]	Printable String
	C	GB	Printable String
Validity	[Per DCC validity period specification]		
Subject	Attribute	Value	Encoding
	CN	[Environment Specific]	Printable String
	OU	[Environment Specific]	Printable String
	C	GB	Printable String
Subject Public Key	ECDSA secp256r1 (OID 1.2.840.10045.3.1.7) according SECG Standard		
Extension	Crit.	Value	
`basicConstraints`	yes	cA: FALSE	
`keyUsage`	yes	`digitalSignature; keyAgreement`	

End Entity Server Certificate

Number of keys: One per environment (HES instance)

Data Field	Value		
Version	v3		
Serial Number	[Automatic no. according to Verisign standard]		
Signature Algorithm	ecdsa-with-SHA256 (OID 1.2.840.10045.4.3.2)		
Issuer	Attribute	Value	Encoding
	CN	Enterprise	Printable String
	O	[Environment Specific]	Printable String
	C	GB	Printable String
Validity	[Per DCC validity period specification]		
Subject	Attribute	Value	Encoding
	CN	[Environment Specific]	Printable String
	OU	[Environment Specific]	Printable String
	O	[Environment Specific]	Printable String
	C	GB	Printable String
Subject Public Key	ECDSA secp256r1 (OID 1.2.840.10045.3.1.7) according SECG Standard		
Extension	Crit.	Value	
`basicConstraints`	yes	cA: FALSE	
`keyUsage`	yes	`digitalSignature; keyAgreement`	
`extKeyUsage`	no	TLS Web Server Authentication	

Application Service Root CA Certificate – Internal Application TLS Chain

Number of Keys: One per CA

Data Field	Value		
version	v3		
Serial number	[Automatic no. according to Verisign standard]		
Signature Algorithm	ecdsa-with-SHA256 (OID 1.2.840.10045.4.3.2)		
Issuer	Attribute	Value	Encoding
	CN	Application Service Root	Printable String
Validity	[Per DCC validity period specification]		
Subject	Attribute	Value	Encoding
	CN	Application Service Root	Printable String
Subject Public Key	ECDSA secp384r1 (OID 1.3.132.0.34) according to SECG Standard		
Extension	Crit	Value	
`basicConstraints`	Yes	cA:TRUE	
`keyUsage`	Yes	`keyCertSign, CRLSign`	

Intermediate Application Service PKI CA Certificate - Internal Application TLS Chain

Number of Keys: One per CA

Data Field	Value		
version	v3		
Serial number	[Automatic no. according to Verisign standard]		
Signature Algorithm	ecdsa-with-SHA256 (OID 1.2.840.10045.4.3.2)		
Issuer	Attribute	Value	Encoding
	CN	Application Service Root	Printable String
Validity	[Per DCC validity period specification]		
Subject	Attribute	Value	Encoding
	CN	Application Service PKI CA	Printable String
Subject Public Key	ECDSA secp384r1 (OID 1.3.132.0.34) according to SECG Standard		
Extension	Crit	Value	
basicConstraints	Yes	cA:TRUE	
keyUsage	Yes	keyAgreement, digitalSignature, keyCertSign	

End Entity PKI Role CA Certificate - Internal Application TLS Chain

Number of Keys: One per CA

Data Field	Value		
version	v3		
Serial number	[Automatic no. according to Verisign standard]		
Signature Algorithm	ecdsa-with-SHA256 (OID 1.2.840.10045.4.3.2)		
Issuer	Attribute	Value	Encoding
	CN	Application Service PKI CA	Printable String
Validity	[Per DCC validity period specification]		
Subject	Attribute	Value	Encoding
	CN	PKI Role CA	Printable String
Subject Public Key	ECDSA secp384r1 (OID 1.3.132.0.34) according to SECG Standard		
Extension	Crit	Value	
`basicConstraints`	yes	cA:FALSE	
`keyUsage`	yes	`keyAgreement, digitalSignature`	

End Entity PKI Role RA Certificate - Internal Application TLS Chain

Number of Keys: One per CA

Data Field	Value		
version	v3		
Serial number	[Automatic no. according to Verisign standard]		
Signature Algorithm	ecdsa-with-SHA256 (OID 1.2.840.10045.4.3.2)		
Issuer	Attribute	Value	Encoding
	CN	Application Service PKI CA	Printable String
Validity	[Per DCC validity period specification]		
Subject	Attribute	Value	Encoding
	CN	PKI Role RA	Printable String
Subject Public Key	ECDSA secp384r1 (OID 1.3.132.0.34) according to SECG Standard		
Extension	Crit	Value	
`basicConstraints`	yes	cA:FALSE	
`keyUsage`	yes	`keyAgreement, digitalSignature`	

12 Annex C: Subscriber Obligations

12.1 Certificate Signing Requests

(A) Each Eligible Subscriber shall ensure that all of the information contained in each Certificate Signing Request made by it is true and accurate.

(B) No Eligible Subscriber may make a Certificate Signing Request which contains:

(i) any information that constitutes a trademark, unless it is the holder of the Intellectual Property Rights in relation to that trademark; or

(ii) any confidential information which would be contained in a Certificate Issued in response to that Certificate Signing Request.

(C) Each Eligible Subscriber shall ensure that the Public Key that is included within a Certificate Signing Request is part of a Key Pair that has been generated using random numbers which are such as to make it computationally infeasible to regenerate that Key Pair even with knowledge of when and by means of what equipment it was generated.

(D) No Eligible Subscriber may make a Certificate Signing Request for the Issue of:

(i) a FOC S1SPKI CA Certificate or FOC S1SP End Entity Certificate which contains the same Public Key as a Public Key which that Eligible Subscriber knows to be contained in any other FOC S1SPKI CA Certificate or FOC S1SPKI End Entity Certificate.

12.2 Use of Certificates and Key Pairs

(A) Each Subscriber shall ensure that it does not use any Certificate, Public Key contained within a Certificate, or a Private Key associated with a Public Key contained in a Certificate, that is held by it other than for the purposes of creating, sending, receiving and processing communications sent to and from SMETS1 Devices, the DCC and the FOC S1SP pursuant to the Code.

12.3 FOC S1SPKI CA and End Entity Certificates: Protection of Private Keys

(A) Each Subscriber shall take reasonable steps to ensure that no Compromise occurs to any:

(i) Private Key which is associated with a Public Key contained in a Certificate for which it is the Subscriber; or

(ii) Secret Key Material associated with that Private Key.

12.4 Certificates: Expiry of Validity Period

(A) Each Subscriber shall, prior to the expiry of the Validity Period of a Certificate for which it is the Subscriber:

(i) request a replacement for that Certificate by applying for the Issue of a new Certificate in accordance with the provisions of this Policy.

13 Annex D: Relying Party Obligations

13.1 Relying Parties

(A) For the purposes of this Policy, a Relying Party in relation to a FOC S1SPKI CA Certificate or a FOC S1SPKI End Entity Certificate means any FOC S1SPKI System, SMETS1 Device or person which relies on the Certificate for the purposes of creating, sending, receiving or processing communications sent to and from the FOC S1SPKI System, the DCC, any person or SMETS1 Device pursuant to this Policy.

(B) For the purposes of Section L13.1, a Relying Party shall be deemed to include:

- (i) in the case of a FOC S1SPKI System which relies on a Certificate, the FOC S1SP; and
- (ii) in the case of a SMETS1 Device which relies on a Certificate, the FOC S1SP.

13.2 Duties in relation to Certificates

(A) Each Relying Party shall:

- (i) before relying on any FOC S1SPKI End Entity Certificate:
  - (a) Check Cryptographic Protection in respect of the FOC S1SP CRL on the relevant FOC S1SPKI Repository; and
  - (b) where that Certificate is shown on the FOC S1SPKI CRL as having been revoked, not rely on the Certificate;
- (ii) before relying on any FOC S1SPCA Certificate:
  - (a) Check Cryptographic Protection in respect of the FOC S1SPKI ARL on the FOC S1SPKI Repository; and
- (iii) where that Certificate is shown on the FOC S1SPKI ARL as having been revoked, not rely on the Certificate;

(B) No Relying Party may rely on a Certificate where the Validity Period of that Certificate has expired.

(C) No Relying Party may rely on a Certificate where it suspects that the Certificate has been Compromised.

(D) Each Relying Party shall take reasonable steps, by means of appropriate Systems, to verify Digital Signatures, Check Cryptographic Protection, Confirm Validity and perform other appropriate cryptographic operations before relying on any Certificate.

14 Annex E: FOC S1SPKI RAPP

14.1 Purpose

(A) This Annex E: FOC S1SPKI RAPP sets out the high-level principal obligations and activities undertaken by the FOC S1SPKI CA in its capacity as the FOC S1SPKI Registration Authority in accordance with this Policy. The FOC S1SPKI RAPP also sets out the activities undertaken by the FOC S1SPKI Registration Authority in support of the procedures as set out in this section.

(B) The FOC S1SPKI CA shall ensure that no Certificate is Issued under this Policy other than to an Eligible Subscriber for a Certificate of the relevant type.

14.2 FOC S1SPKI RAPP Principles

(A) All Certificates requested and Certificates issued under the auspices of the FOC S1SPKI CA must be:

(i) compliant with PKCS#10;
(ii) BER encoded;
(iii) compliant with the Certificate Profiles as set out in Appendix B of this Policy; and
(iv) compliant with the obligations as set out in Annex C of this Policy.

14.3 FOC S1SPKI Registration Authority Roles

(A) The FOC S1SPKI RA consists of the following roles:

(i) The Intermediate Operator CA performing the technical RA role for automatically approving End Entity Operator Device Certificates for issuance (as requested by the FOC S1SP HES on behalf of the SMETS1 Device);
(ii) FOC S1SPKI RA Personnel submitting and approving all other Certificates for issuance.

(B) Only FOC S1SPKI RA Personnel with Privileged User rights can submit and approve Certificates on behalf of Eligible Subscribers using the FOC S1SPKI CA Systems. This is enforced through:

(i) Pre-authorised and pre-approved access to FOC S1SPKI CA Systems;
(ii) Access control to the FOC S1SPKI CA Systems;
(iii) User account management (audit and logging);
(iv) Dedicated named accounts on the FOC S1SPKI CA System;

(C) Prior to being granted access to FOC S1SPKI CA Systems, all such FOC S1SPKI RA Personnel with Privileged User rights will either have:

(i) identities checked in line with personnel security standard BS7858; and/or
(ii) /background clearance checks performed in accordance with this Policy and the FOC S1SPKI CPS.

14.4 Authorised Subscribers

(A) The following are Authorised Subscribers under this Policy:
(B) a SMETS1 Device with which the FOC S1SP is to communicate;
(C) the FOC S1SP HES;
(D) the FOC S1SPCA;
(E) the Application Service CA; and
(F) FOC S1SPKI Personnel (acting on behalf of the FOC S1SP).
(G) At the point of the FOC S1SPKI RA approving the above, then it (or they) become an Authorised Subscribers.

14.5 Eligible Subscribers

(A) Where it is, or they are, an Authorised Subscriber, the following is/are an Eligible Subscriber in respect to the specified Certificates:

(i) the FOC S1SP HES which is an Eligible Subscriber for the following FOC S1SP End Entity Certificates only:

   (a) End Entity Server Certificate; or
   (b) End Entity Push Certificate;
(ii) the FOC S1SPCA is an Eligible Subscriber for all FOC S1SPCA Certificates.
(iii) SMETS1 Devices are Eligible Subscribers for the following FOC S1SP End Entity Certificate only:
   (a) End Entity Operator Device Certificate.
(iv) The Application Service CA which is an Eligible Subscriber for the following Application CA Certificates only:
   (a) Application Service Root CA Certificate;
   (b) Intermediate Application Service PKI CA Certificate.
(v) FOC S1SPKI Personnel, who are Eligible Subscribers for End Entity PKI Role RA Certificates only.
(vi) S1SPKI CA Systems which is are only Eligible Subscriber for End Entity PKI Role CA Certificates.

14.6 FOC S1SPKI Technical RA Verification and Issuance of Certificates

(A) For personnel controls, resources providing trust services, have either SC or BS7858 Clearance and training for the provisioning of digital certificates.

(B) All relevant personnel are security cleared and trained to manage the provisioning of digital certificates. The overall management of the vetting process is provided by the relevant Secure Vetting Team, liaising directly with the Account Security Officer at DCC.

Comments	Manual Certificate Generation	Automated Certificate Generation
(A) Both the Intermediate Enterprise CA and the Intermediate Operator CA are subscribers of Certificates that are Issued by the Operator Root CA which is operated by Capgemini. Another subscriber includes the Comms Hub as Certificates are issued to it by the Intermediate Operator CA. (B) The Intermediate Operator CA performs the following technical RA check in response to a Certificate Signing Request. I. An Operator Device Certificate (ODC) is issued to each Comms Hub. The Certificates are signed by the Intermediate Operator CA, with the Head End acting as a registration authority and delivering these Certificates to the Comms Hub. Each Comms Hub will	Before sending the CSR the file must be encrypted with the requestors GPG public key and signed with the senders own GPG key. This will allow the sender to validate the encryption before sending. Once encrypted the file is emailed to the requesting party representative.	Certificate changes take place under the governance of the Head End System. In its capacity as the Registration Authority it determines whether a Certificate needs to be issued and manages the creation of the CSR, rather than the end-device deciding that a Certificate needs to be issued and requesting the RA to forward a CSR to the CA. The Head End System will have established that it is communicating with a trusted device before if performs any Certificate operations. This uses the chain of trust that the Head End System has been explicitly configured with.

Comments	Manual Certificate Generation	Automated Certificate Generation
have its own ODC and Private Key, and the Head End will hold a copy of all ODCs. Each Comms Hub uses its ODC to identify itself during TLS session setup. The Certificate Signing Request is sent to a production central system (which incorporates the FOC S1SP CA Operator CA) in PKCS#10 file format. II. The Operator CA verifies the Certificate Signing Request as well as performing a proof of possession check using the PKCS#10 format. III. When the Operator CA verifies the CSR, then: a. it passes the CSR to the Comms Hub to process the Certificate Signing Request; b. If all verification checks are successful, the Comms Hub stores the Certificate chain and its own internal storage.		

14.7 Revocation of a Certificate

14.7.1 General Organisation Certificate revocation obligations

(A) The FOC S1SP shall permit each of the following individuals to request the revocation of a Certificate, where the reasons for such revocation request must be one of the permitted reasons for Certificate revocation as set out in Part 4.9 of this Policy:

(B) Any FOC S1SP ITSC member, on behalf of the FOC S1SP ITSC;

(C) Any Subscriber for a Certificate; or

(D) Any FOC S1SPKI RA Personnel, on behalf of the FOC S1SP.

(E) The FOC S1SP, in its role as FOC S1SPKI Registration Authority, shall only accept CRR via a secured electronic means as set out in this Annex E;

(F) The revocation of a Certificate shall be permanent and the FOC S1SPKI Registration Authority shall ensure that no revoked Certificate may be reinstated.

(G) The FOC S1SP shall, each month, prepare and submit a report to the DCC regarding the number and nature of Certificate revocations.

14.7.2 Procedure for Certificate Revocation

(A) The procedure for authorisation, verification and, where verified, revocation of Certificates is as set out immediately below.

(B) As soon as reasonably practicable when Certificate revocation is required:

(i) An individual as per 14.7.1 (A) of this Annex E shall submit, using the mechanisms set out in 14.7.1 (B) of this Annex E, a CRR to the FOC S1SPKI Registration Authority.

(ii) The reason for such CRR shall be one of the permitted reasons for Certificate revocation as set out in Section 4.9 of this Policy.

(iii) Each CRR shall contain the following information:

(a) Identity of the Subscriber;

(b) Unambiguously (i.e. by specifying the serial number of the Certificate) identification of the Certificate to be revoked; and

(c) The reason for the Certificate revocation.

(C) Upon receipt of the CRR, the FOC S1SPKI RA Personnel on behalf of the FOC S1SPKI RA shall, as soon as reasonably practicable:

(i) Verify and authenticate the CRR; and

(ii) Where verified and authenticated successfully, approve and then process the CRR; or

(iii) Where the CRR cannot be successfully verified and authenticated:

(a) Reject the CRR; and

(b) Inform the individual making the CRR of such rejection; and

(c) Immediately notify the FOC S1SP ITSC and the DCC of failed CRR attempts.

(D) The FOC S1SPKI RA shall, as soon as reasonably practicable following a successful CRR:

(i) Revoke the identified Certificate that is the subject of the CRR;

(ii) Update the relevant FOC S1SPKI ARL or FOC S1SPKI CRL and publish such ARL or CRL to the FOC S1SPKI Repository, as set out in this Policy; and

(iii) Notify the FOC S1SP and the DCC of the successfully revocation of the Certificate in the CRR.

(E) The FOC S1SPKI Registration Authority shall treat each CRR and any associated circumstances as confidential.

(F) The FOC S1SPKI RA shall ensure that no single individual can request and subsequently approve a CRR.

14.8 Certificate Rotation

(A) Prior to the expiry of the validity period of a given Certificate the Registration Authority (Head End [automated] and system operator [manual]) must request a new Certificate by applying for the Issuance of a new Certificate in accordance with the provisions of this Policy.

SEC Appendix AQ

SEC Variation Testing Approach Document for the CH&N Arrangements

Table of Contents

1. Definitions and Interpretation

1.1. In this SEC Variation Testing Approach Document for CH&N SEC Variations (this “CH&N SVTAD”), except where the context otherwise requires, the expressions in the left-hand column within Table 1.1 shall have the meanings given to them in the right-hand column within Table 1.1. Where not defined in this CH&N SVTAD, words beginning with a capital letter used in this document are defined in Section A of the SEC.

1.2. Where there are conflicts between this CH&N SVTAD and any related CH&N Test Approach Document or CH&N Test Coverage Document, this CH&N SVTAD shall take precedence.

1.3. Where obligations are expressed in respect of DCC Service Providers in this CH&N SVTAD, a CH&N Test Approach Document or a CH&N Test Coverage Document, these shall be construed as obligations on the DCC. Where text is included in this CH&N SVTAD, a CH&N Test Approach document or a CH&N Test Coverage Document which does not explicitly place obligations on a Party, the Panel, or Testing Participant, these shall be construed as obligations on the DCC.

Table 1.1 CH&N SVTAD Definitions

Term	Meaning
CH&N Arrangements	means arrangements for utilising the newer forms of next-generation wireless mobile telecommunications technology for the secure telecommunications platform used (or to be used) for the purposes of communicating with Enrolled Smart Metering Systems.
CH&N Mandated User Testing Document	means any document prepared pursuant to Clause 6 that sets out the approach to mandatory User Testing.
CH&N Release	means those changes to all or part of the DCC Total System that are planned to be implemented at the same time, as set out in the Joint Industry Plan, and which are necessary to support the delivery of the CH&N SEC Variations.
CH&N SEC Variations	means the variations to the SEC that are planned to support the introduction of and transition to the CH&N Arrangements as published by the DCC and/or the Secretary of State from time to time.

Term	Meaning
CH&N Solution	means the Sub-Systems delivered or changed for the purposes of the CH&N SEC Variations, including the Data Services Provider Sub-System, the 4G Communications Hubs (4GCH), Device Manager(s), Order Management System(s), Logistics, and the associated part of the SM WAN that will comprise 4G mobile communications technology.
CH&N Test Approach Document	means a document produced pursuant to Clause 4.1.
CH&N Test Coverage Document	means a document produced pursuant to Clause 4.2.
Completion Report	means a report that is produced setting out evidence demonstrating how the criteria for the completion of testing has been met.
Component Integration Test Stage	means a test stage focusing on verifying individual interactions between Sub-Systems.
Data Services Provider, or DSP	means the DCC acting from those systems identified in part a) of the definition of DCC Live Systems.
Device Manager	means a Sub-System utilised, amongst other things, to manage the interactions between the 4GCH and the rest of the Modified DCC Total System.
Joint Industry Plan (JIP)	means the part of the joint industry plan that is agreed at the Department for Energy, Security and Net Zero's smart metering design group that relates to the 4G Communications Hubs and Network Programme.
June 2024 SEC Release	means the SEC Release planned to go live in June 2024.
Link Test Stage	means a test stage focusing on the testing of interfaces and interactions within a Sub-System.
Logistics	means a Sub-System utilised to manage the logistics processes for the delivery of 4GCH.

Term	Meaning
Modified DCC Total System	means the DCC Total System as will be modified as a result of each CH&N Release.
Order Management System(s)	means a Sub-System utilised to manage the forecasting, ordering and manufacturing process for 4GCHs.
Pre-Integration Test Phase (“PIT”)	means the test phase that is inclusive of the Unit Test Stage, Link Test Stage, System Test Stage for a new or change to a Sub-System. Optionally PIT may also include a Component Integration Test Stage.
Sub-System	means an element of the Modified DCC Total System, in respect of which changes will be tested independently for the purposes of the Unit Test Stage, Link Test Stage, and System Test Stage .
System Test Stage	means a test stage focusing on verifying that a Sub-System as a whole meets specified requirements.
Systems Integration Test Phase (“SIT”)	means the test phase focusing on verifying the end-to-end operation of the Modified DCC Total System that will exist as a result of the CH&N Release that is the subject of the test phase.
TAG	means the Panel’s Testing Advisory Group.
Testing Baselines Requirements document (“TBRD”)	a document published by the Secretary of State from time to time setting out baseline versions of the Smart Energy Code for the purposes of test exit decisions
Testing Issue Thresholds	means the maximum number of extant Testing Issues that may be permitted at completion of a test phase.
Unit Test Stage	means a test stage focusing on the testing of individual hardware or software components within a Sub-System.

Term	Meaning
User Testing	means testing by one or more Users of all or part of any changes to the Modified DCC Total System in respect of a CH&N Release.

2. General

2.1. This document is the SEC Variation Testing Approach Document for the CH&N SEC Variations.

2.2. Section X11.7 of the Code requires that the DCC and each person other than the DCC that participates in (or is required to participate in) testing under a SEC Variation Testing Approach Document shall comply with the SEC Variation Testing Approach Document.

2.3. Section X11.8 of the Code specifies that Section H14 of the Code (Testing Services) and the Enduring Testing Approach Document shall apply in respect of testing under a SEC Variation Testing Approach Document as if such testing was a Testing Service under Section H14.34 (Modification Implementation Testing); and each participant in such testing shall be deemed to be a Testing Participant for such purposes.

2.4. This CH&N SVTAD sets out:

(a) the framework for the testing that is required to be undertaken for the introduction of the CH&N SEC Variations;

(b) the arrangements that apply to the development of CH&N Testing Approach Document(s) for each CH&N Release;

(c) the arrangements that apply to the development of CH&N Test Coverage Document(s) for each CH&N Release; and

(d) the rules to apply to the development of any CH&N Mandated User Testing Document(s) for each CH&N Release; and

(e) the rules to apply to the development of a methodology for the selection of devices to be used in testing.

2.5. Each of the documents described in Clause 2.4 (b)-(d) may be produced:

(a) as separate documents for the version of the Modified DCC Total System that will exist for each CH&N Release;

(b) as separate documents for each of PIT and SIT in respect of a CH&N Release;

(c) in the case of PIT for a CH&N Release, as separate documents per Sub-System; or

(d) as any combination of the aforementioned permutations,

as the DCC considers appropriate. Each document shall clearly state the CH&N Release(s) to which it pertains, and where combined, the DCC shall state in the combined document the individual parts of which it is comprised.

2.6. Testing undertaken pursuant to this CH&N SVTAD shall be performed by the DCC and any other Party that participates in it in accordance with Good Industry Practice.

2.7. The DCC shall not commence any tests in respect of a CH&N Release (including for individual Sub-Systems in PIT) until the CH&N Test Approach Document(s) and CH&N Test Coverage Document(s) that set out the approach to and coverage of those tests has been approved by the TAG.

2.8. Where the CH&N Test Approach Document produced pursuant to Clause 4.1.1 does not set out the approach to the entirety of testing that will be undertaken during the test phase to which the document relates (PIT and/or SIT) in respect of a CH&N Release, this shall be clearly stated in the CH&N Test Approach Document. The DCC shall subsequently seek TAG approval of an updated CH&N Test Approach Document(s) as and when the remaining approach to testing is planned. As set out in Clause 2.7, the DCC shall not commence any tests without a CH&N Test Approach Document setting out the approach to those tests having been agreed pursuant to Clause 4.1.2 or 4.1.4.

2.9. Where the CH&N Test Coverage Document produced pursuant to Clause 4.2.1 does not set out coverage of the entirety of testing that will be undertaken during the test phase to which the document relates (PIT and/or SIT) in respect of a CH&N Release, this shall be clearly stated in the CH&N Test Coverage Document. The DCC shall subsequently seek TAG approval of an updated CH&N Test Coverage Document(s) as and when remaining tests are planned. As set out in Clause 2.7, the DCC shall not commence any tests without a CH&N Test Coverage Document agreed pursuant to Clause 4.2.2 or 4.2.4 setting out the coverage of those tests.

Timetable for Testing

2.10. Test phases shall be commenced in the timescales that are necessary to facilitate testing in accordance with the milestones on the Joint Industry Plan.

CH&N Testing Objective

2.11. The objective of testing undertaken pursuant to this CH&N SVTAD (the “CH&N Testing Objective”) is to demonstrate that the DCC and the component parts of the Modified DCC Total System in respect of each CH&N Release operate and interoperate with User Systems and Smart Metering Systems to the extent necessary for the DCC to comply with the relevant requirements that will exist in the SEC that pertain to that CH&N Release.

Test Entry Criteria

2.12. The fulfilment of the following Entry Criteria is required to permit entry into PIT for a Sub-System or SIT in respect of each CH&N Release:

(a) test plan signed off by the DCC;

(b) all relevant Testing Approach Documents and Test Coverage Documents approved by the TAG;

(c) Test Completion Certificates for any precursor test phase issued;

(d) test specification prepared, including the production of a test traceability matrix;

(e) confirmation that the required test laboratories, Devices, tools, stubs, environments and data are in place, secure and are ready for testing; and

(f) an approval to proceed certificate for the test phase has been issued by the DCC.

3. Modification of the CH&N SVTAD

3.1. This CH&N SVTAD:

(a) shall be modified by the DCC in accordance with any direction to do so made by the Secretary of State. The DCC shall consult with Parties concerning any proposed modification to this document in accordance with any direction to do so by made by the Secretary of State;

(b) may be modified by the DCC following consultation with Parties and other relevant persons, the TAG, the Authority, and the Secretary of State, provided that:

i. prior to making any such modification, DCC must present to the Secretary of State a summary of the consultation responses received and an explanation of how the DCC has taken them into account; and

ii. it may not be modified to the extent that the Secretary of State directs otherwise; and

(c) may be modified by DCC without consultation where the modification is of a minor typographical nature, or where the modification does not have any material effect on the rights or obligations of SEC Parties or any other person who is entitled to undertake testing in accordance with this document.

4. Creation and Modification of the CH&N Test Artefacts

4.1. CH&N Testing Approach Document(s)

4.1.1. Subject to Clause 6, the DCC shall produce each CH&N Test Approach Document(s) in accordance with the requirements in Clause 2.5, which shall include the approach to testing for Sub-Systems in PIT and for the Modified DCC Total System within SIT in respect of each CH&N Release including:

(a) the proposed amendments to this Code that are the subject of or which pertain to the testing, an explanation of the associated changes to the DCC Total System, and the testing objective;

(b) the scope of the CH&N Release(s) to which the Testing Approach Document relates;

(c) the principles and approach to apply to PIT(s) and SIT(s);

(d) the testing environments to be used;

(e) whether devices are to be used in PIT and/or SIT for a CH&N Release and if so, the applicable CH&N Device Selection Methodology;

(f) ~~the process to be followed in selecting devices for use in PIT(s) and SIT(s)~~;

(g) the process for resolving Testing Issues, the applicable Testing Issue Thresholds for use in the relevant PIT completion(s) and relevant SIT completion(s) and the process for excluding Testing Issues;

(h) the exit criteria for testing to complete successfully for the relevant PIT and for the relevant SIT;

(i) any perceived risks associated with the approach to testing and the proposed mitigations;

(j) the approach to providing for assurance of the testing undertaken; and

(k) matters to be included in any Completion Reports for the relevant PIT. The DCC may combine a PIT Completion Report in respect of a CH&N Release for a Sub-System with other PIT Completion Reports in respect of other CH&N Releases pertaining to the same Sub-System, and where it does so, this shall be clearly stated in the combined Completion Report; and

(l) matters to be included in any Completion Report for the relevant SIT in respect of the CH&N Release.

4.1.2. The DCC shall submit each draft CH&N Testing Approach Document in respect of a CH&N Release to the TAG for review (and such submission by the DCC and review by the TAG may take place prior to this Clause 4.1.2 coming into effect); and:

(a) where the TAG and the DCC can reach an agreement, the relevant draft CH&N Testing Approach Document shall be updated by the DCC as necessary and deemed to be final; or

(b) where the TAG and the DCC cannot reach an agreement, the matters of disagreement shall be referred by the DCC to the Secretary of State for determination. The Secretary of State's decision on such matters shall be final and binding for the purposes of this Code and the relevant draft CH&N Testing Approach Document shall be updated by the DCC as necessary and deemed to be final.

4.1.3. The DCC shall comply with each CH&N Testing Approach Document in respect of a CH&N Release.

4.1.4. Revisions to a CH&N Testing Approach Document finalised pursuant to Clause 4.1.2:

(a) may, from time to time, be submitted by the DCC to the TAG for agreement in accordance with the provisions of Clause 4.1.1, and the provisions of Clause 4.1.1 shall apply (again) to the revised version of the document; or

(b) shall be made by the DCC in accordance with any direction to do so issued by the Secretary of State. The DCC shall consult with TAG concerning any such proposed revision in accordance with any direction to do so issued by the Secretary of State.

4.2. CH&N Test Coverage Document(s)

4.2.1. Subject to Clause 6, the DCC shall prepare each CH&N Test Coverage Document in accordance with the requirements in Clause 2.5, which shall set out the depth and breadth of testing required in the relevant PITs and relevant SIT in respect of a CH&N Release and shall include:

(c) the scope (breadth) and coverage (depth) of testing against requirements for the relevant Sub-System (in the case of PIT) and the Modified DCC Total System (in the case of SIT), identified as groupings of functional and non-functional requirements;

(d) where a Test Coverage Document covers both a PIT test phase and SIT, whether the identified requirement shall be tested in PIT or SIT;

(e) where the TAD in respect of PIT or SIT for the CH&N Release specifies that Devices will be used in testing, the list of Devices selected to be utilised in the relevant PIT or relevant SIT (as the case may be), pursuant to the applicable CH&N Device Selection Methodology referenced in the TAD ; and

(f) any perceived risks associated with the scope and coverage of testing and the proposed mitigations.

4.2.2. The DCC shall submit each draft CH&N Test Coverage Document in respect of a CH&N Release to the TAG for review (and such submission by the DCC and review by the TAG may take place prior to this Clause 4.2.3 coming into effect) and:

(a) where the TAG and the DCC can reach an agreement, the relevant draft CH&N Test Coverage Document shall be updated by the DCC as necessary and deemed to be final; or

(b) where the TAG and the DCC cannot reach an agreement, the matters of disagreement shall be referred by the DCC to the Secretary of State for determination. The Secretary of State's decision on such matters shall be final and binding for the purposes of this Code and the relevant draft CH&N Test Coverage Document shall be updated by the DCC as necessary and deemed to be final.

4.2.3. The DCC shall comply with each CH&N Test Coverage Document in respect of a CH&N Release and shall take all reasonable steps to complete the tests set out in each CH&N Test Coverage Document in accordance with the milestones on the Joint Industry Plan.

4.2.4. Revisions to a CH&N Test Coverage Document finalised pursuant to Clause 4.2.3:

(a) may, from time to time, be submitted by the DCC to the TAG for agreement in accordance with the provisions of Clause 4.2.3, and the provisions of Clause 4.2.3 shall apply (again) to the revised version of the document; or

(b) shall be made by the DCC in accordance with any direction to do so issued by the Secretary of State. The DCC shall consult with TAG concerning any such proposed revision in accordance with any direction to do so issued by the Secretary of State.

4.3. CH&N Device Selection Methodology (CH&N DSM)

4.3.1. Subject to Clause 4.3.2 and 4.3.3, the DCC shall prepare a document (the "CH&N Device Selection Methodology") for each CH&N Release which shall set out the process to be followed to select devices to be used for testing in the relevant Sub-System PITs and relevant SIT in respect of that CH&N Release.

4.3.2. A new CH&N DSM does not need to be prepared by the DCC where:

(a) the relevant Testing Approach Document for PIT and/or SIT in respect of a CH&N Release states that an existing CH&N DSM shall apply, or

(b) where the CH&N Release is not required to test with any Device, as set out in the Testing Approach Document for that CH&N Release.

4.3.3. ACH&N Device Selection Methodology shall not apply to testing for the CH&N Release that comprises part of the June 2024 SEC Release that is tested pursuant to Clause 6. Instead, the

DCC shall run tests for that CH&N Release using the devices set out in the test approach document for the June 2024 SEC Release.

4.3.4. The DCC shall submit each CH&N Device Selection Methodology to the TAG for review (and such submission by the DCC and review by the TAG may take place prior to this Clause 4.3.3 coming into effect) and:

(a) where the TAG and the DCC can reach an agreement, the relevant draft CH&N Selection Methodology shall be updated by the DCC as necessary and deemed to be final; or

(b) where the TAG and the DCC cannot reach an agreement, the matters of disagreement shall be referred by the DCC to the Secretary of State for determination. The Secretary of State's decision on such matters shall be final and binding for the purposes of this Code and the relevant draft CH&N Device Selection Methodology shall be updated by the DCC as necessary and deemed to be final.

4.3.5. Revisions to any CH&N Device Selection Methodology finalised pursuant to Clause 4.3.3:

(a) may, from time to time, be submitted by the DCC to the TAG for agreement in accordance with the provisions of Clause 4.3.3, and the provisions of Clause 4.3.3 shall apply (again) to the revised version of the document; or

(b) shall be made by the DCC in accordance with any direction to do so issued by the Secretary of State. The DCC shall consult with TAG concerning any such proposed revision in accordance with any direction to do so issued by the Secretary of State.

5. <u>Test Completion for PIT and SIT in respect of a CH&N Release</u>

5.1. Completion of testing for:

(a) PIT for each relevant Sub-System in respect of a CH&N Release; and

(b) SIT in respect of a CH&N Release,

shall, in each case, only complete when the Panel determines that the exit criteria for completion as set out in the relevant Testing Approach Document have been met.

5.2. When the DCC considers that such completion ought to occur, the DCC shall prepare a Completion Report as provided for in the relevant CH&N Testing Approach Document. The DCC shall:

(a) notify the Secretary of State, the Authority, the Panel, and the Parties that the DCC considers that testing has been completed for the test phase and, in the case of PIT, Sub-System in question in respect of the CH&N Release;

(b) provide the Authority, the Panel, and the Secretary of State with copies of the Completion Report and a list of the sections of such report that the DCC considers should be redacted prior to publication; and

(c) review the supporting documentation and evidence with regards to the relevant exit criteria with the TAG.

5.3. The Panel shall confirm the completion of testing for PIT for a Sub-System in respect of a CH&N Release and SIT in respect of a CH&N Release (as the case may be), or shall highlight where it believes the exit criteria have not been met.

5.4. Where the Panel confirms the completion of testing for the relevant test phase (subject to the Panel and the DCC reaching an agreement regarding resolution of any issues raised by the Panel) the Completion Report shall be updated by the DCC as necessary and deemed to be final.

5.5. Where the Panel declines to confirm the completion of testing for the relevant test phase, the DCC shall update the relevant Completion Report to reflect resolution of any issues where the DCC and the Panel reached an agreement, and the DCC shall then either:

(a) refer the matters where the Panel and the DCC are in disagreement to the Secretary of State for determination; or

(b) continue with testing (and Clause 5.2 shall apply again).

5.6. Where a referral has been made by the DCC pursuant to Clause 5.5, the determination of the Secretary of State shall be final and binding for the purposes of this Code as follows:

(a) where the Secretary of State agrees that testing for the relevant test phase is complete, the relevant Completion Report shall be updated by the DCC as necessary, and the contents shall be deemed to be final; or

(b) where the Secretary of State disagrees that testing for the relevant test phase is complete, the DCC shall continue with testing (and Clause 5.2 onwards shall apply again).

5.7. The DCC shall publish the final Completion Reports for the relevant test phase as soon as reasonably practicable, which shall be anonymised and redacted where directed by the Panel, on the DCC Website. The DCC shall notify the Panel, the Secretary of State, the Authority, and the SEC Parties of the publication of the reports.

6. <u>Dual Testing Governance for SEC Modifications and CH&N SEC Variations in the same SEC Release</u>

6.1. It is acknowledged that the CH&N SEC Variations required to Appendix AD (the DCC User Interface Specification) are planned to be implemented as part of the June 2024 SEC Release. Rather than producing a CH&N Test Approach Document and a CH&N Test Coverage Document in respect of those CH&N SEC Variations, the DCC shall provide for all of the matters that would normally be set out under those documents in respect of the CH&N SEC Variations to Appendix AQ be set out in a test approach document to be agreed by the TAG that also includes testing of the Modifications that comprise the June 2024 SEC Release, provided that:

(a) the entry criteria set out in Clause 2.10 shall apply in respect of the CH&N SEC Variations comprising part of the June 2024 SEC Release, and

(b) where the TAG and the DCC cannot reach an agreement on the approach to and/or coverage of the testing for the CH&N SEC Variations, the matters of disagreement shall be referred by the DCC to the Secretary of State for determination. The Secretary of State's decision on such matters shall be final and binding for the purposes of this Code and the June 2024 SEC Release testing approach document shall be updated by the DCC as necessary and deemed to be final in respect of the CH&N SEC Variations.

6.2. The DCC shall comply with the test approach document for the June 2024 SEC Release insofar as it relates to the CH&N Variations.

6.3. The provisions of Clause 5 shall apply in respect of completion of testing of the CH&N Variations that comprise part of the June 2024 SEC Release, including that where the Panel and the DCC cannot reach an agreement on whether testing has completed in respect of the CH&N SEC Variations, the matters of disagreement shall be referred to the Secretary of State for determination. It is acknowledged that the Completion Report in respect of the CH&N SEC Variations comprising part of the June 2024 Release shall form part of the Completion Report for the June 2024 SEC Release.

7. Mandatory User Testing (if Required)

7.1. Where the DCC considers that User testing is required prior to implementation of a CH&N Release, it shall set out its proposals for User testing in a draft CH&N Mandated User Testing Document for the CH&N Release, including those Users that should be required to participate in the testing and the User Role in which they are required to participate; the entry requirements for those Users required to participate in the testing, the approach to testing; the arrangements for test completion; the process for resolving testing disputes; and notification of test completion. In developing any CH&N Mandated User Testing Document, the DCC shall consult with the TAG, Parties, and other relevant stakeholders prior to the submission of the document to the Secretary of State.

7.2. Following consultation under Clause 7.1, the DCC shall submit each draft CH&N Mandated User Testing Document to the Secretary of State, indicating:

(a) why the DCC considers the draft to be fit for purpose;

(b) copies of the consultation responses received; and

(c) any areas of disagreement that arose during the consultation process and that have not been resolved.

7.3. The DCC shall comply with any direction given by the Secretary of State to re-consider, re-consult, and/or re-submit the draft document(s).

7.4. Should a CH&N Mandated User Testing Document be approved by the Secretary of State for a CH&N Release, the DCC and each Party other than the DCC that participates in (or is required to participate in) testing, as set out in such approved document, shall comply with that CH&N Mandated User Testing Document for that CH&N Release.

8. Interoperability Issues arising in UIT environments

8.1. Prior to the completion of the LSC volume manufacturing milestone set out in the Joint Industry Plan, where interoperability Testing Issues arise during testing in environments used for User testing between the Communications Hub(s) and other HAN-connected Devices, the DCC shall triage and investigate the issue (in conjunction with relevant experts both internal and external) and:

(a) where the DCC determines that the Communications Hub is non-compliant with the baseline version of the SEC specified in the Testing Baseline Requirements Document ("TBRD"), the DCC shall take the steps necessary to rectify and close the issue, or

(b) where the DCC considers that the Communications Hub is compliant with the baseline version of the SEC specified in the TBRD, the DCC shall provide to the Secretary of State a description of what the issue is and the results of its investigation, including a view of how the issue should be rectified and shall refer the matter to the Secretary of State for consideration. The Secretary of State shall determine how the Testing Issue should be rectified and shall notify its decision to the DCC and other stakeholders.

Version AR1.0

APPENDIX AR

SEC Variation Testing Approach Document for the Enduring Change of Supplier Arrangements

Contents

1 Definitions and Interpretations

1.1 In this SEC Variation Testing Approach Document for the Enduring Change of Supplier (ECoS) Arrangements (this "**ECOS SVTAD**"), except where the context otherwise requires, the expressions in the left-hand column within Table 1.1 shall have the meanings given to them in the right-hand column within Table 1.1. Where not defined in this ECoS SVTAD, words beginning with a capital letter used in this document are defined in Section A of the SEC.

1.2 Where there are conflicts between this ECoS SVTAD and the related ECoS Testing Approach Document, this ECoS SVTAD shall take precedence.

1.3 Where obligations are expressed in respect of DCC Service Providers in this ECoS SVTAD, these shall be construed as obligations on the DCC. Where text is included in this ECoS SVTAD which does not explicitly place obligations on a Party, the Panel, or Testing Participant, these shall be construed as obligations on the DCC.

Table 1.1 ECOS SVTAD Definitions

Term	Meaning
Centralised Registration Service (CRS) (aka Central Switching Service)	has the meaning given to this term in Part C of Condition 15 of the DCC Licence.
Completion Report	means a report that is produced setting out evidence demonstrating how the criteria for the completion of the testing has been met.
ECoS	the abbreviation for Enduring Change of Supplier.
ECoS Testing Approach Document	means the testing approach document produced pursuant to Clauses 3.2 – 3.5 of this document.
ECoS Mandated User Testing Document	means any document prepared pursuant to Clause 3 of this document that sets out the approach to mandatory User Testing.
ECoS Certificate	means an Organisation Certificate for which the ECoS Service Provider is the Subject.

ECoS Migration	means, in relation to a Device (or a number of Devices), the replacement of those Device Security Credentials held on or in relation to that Device (or those Devices) that have been populated with information from a TCoS Certificate with information from an ECoS Certificate and any supporting arrangements. The term "ECoS Migrated" shall be interpreted accordingly.
ECoS Service Provider	means the DCC Service Provider(s) that will support the operation of the CoS Party following the completion of the implementation of the Enduring Change of Supplier Arrangements.
Enduring Change of Supplier (ECoS) Variations	means the variations to the SEC that are planned as part of the introduction of the ECoS Arrangements, including, for the avoidance of doubt, those changes that will apply during the period of ECoS Migration. The variations shall, except to the extent agreed by the Secretary of State, additionally include those changes to the SEC that the Authority plans to make as part of the introduction of the Centralised Registration Service and which relate to the sending of Registration Data to the CoS Party.
Enduring Change of Supplier Arrangements (ECoS Arrangements)	has the meaning given to this term in Condition 13A of the DCC Licence.
Exit Criteria	means the criteria that must be met in order for testing (or a phase of testing) to complete.
Modified DCC Total System	means the DCC Total System as will be modified to enable the delivery of Services following the introduction of the ECoS Arrangements.
Subject	has the meaning given to that term in Appendix B of the SEC (Organisation Certificate Policy).
TAG	means the SEC Panel's Testing Advisory Group.
TCoS	the abbreviation for transitional change of supplier.
TCoS Certificate	means an Organisation Certificate for which the TCoS Service Provider is the Subject.
TCoS Service Provider	means the DCC Service Provider that solely supported the operation of the CoS Party prior to the commencement of the implementation of the Enduring Change of Supplier Arrangements.

Testing Issue Thresholds	means the maximum number of extant Testing Issues that may be permitted at test completion.
User Testing	means testing by one or more Users of all or part of any changes to the Modified DCC Total System that occur as a result of the ECoS Arrangements

2 General

2.1 This document is the SEC Variation Testing Approach Document for the ECoS Variations.

2.2 Section X11.7 of the Code requires that the DCC and each person other than the DCC that participates in (or is required to participate in) testing under a SEC Variation Testing Approach Document shall comply with the SEC Variation Testing Approach Document.

2.3 Section X11.8 of the Code specifies that Section H14 of the Code (Testing Services) and Appendix J of the Code (Enduring Testing Approach Document) shall apply in respect of testing under a SEC Variation Testing Approach Document as if such testing was a Testing Service under Section H14.34 (Modification Implementation Testing); and each participant in such testing shall be deemed to be a Testing Participant for such purposes.

2.4 This ECoS SVTAD sets out:

(a) the framework for the testing that is required to be undertaken for the introduction of the ECoS Variations;

(b) the arrangements that apply to the development of the ECoS Testing Approach Document; and

(c) the rules to apply to the development of any ECoS Mandated User Testing Document.

2.5 This ECoS SVTAD shall be modified by the DCC in accordance with any direction to do so made by the Secretary of State. The DCC shall consult with Parties concerning any proposed modification to those documents in accordance with any direction to do so made by the Secretary of State.

2.6 The ECoS Testing Approach Document shall be modified by the DCC in accordance with any direction to do so made by the Secretary of State. Any such modifications shall be submitted by the DCC to the TAG for agreement in accordance with the provisions of Clause 3.3, and the provisions of Clause 3.4 shall apply (again) to the revised version of the document.

2.7 This ECoS SVTAD may be modified by the DCC following consultation with Parties and other relevant persons, the TAG, the Authority, and the Secretary of State, provided that:

(a) prior to making any such modification, the DCC must present to the Secretary of State a summary of the consultation responses received and an explanation of how the DCC has taken them into account; and

(b) may not be modified to the extent that the Secretary of State directs otherwise.

2.8 The ECoS SVTAD may be modified by DCC without consultation where the modification is of a minor typographical nature, or where the modification does not have any material effect on the rights or obligations of SEC Parties or any other person who is entitled to undertake testing in accordance with this document.

3 ECoS Testing Approach Documents

3.1 Testing undertaken pursuant to this ECoS SVTAD shall be performed by the DCC and any other Party that participates in it in accordance with Good Industry Practice.

3.2 The DCC shall prepare a draft ECoS Testing Approach Document, which may include the approach to testing where it is required for the changes that comprise part of the ECoS Variations including:

(a) the proposed amendments to this Code that are the subject of the testing, an explanation of the associated changes to the Modified DCC Total System, and the testing objective;

(b) the testing environments to be used;

(c) the requirements (if any) for device testing;

(d) the requirements (if any) for security testing;

(e) the requirements (if any) for system capacity testing;

(f) the testing that shall be undertaken, both in terms of the scope of testing and the extent of testing (including negative tests) and the approach to regression testing;

(g) the requirements for ECoS Migration testing;

(h) the applicable Testing Issue Thresholds and the process for excluding Testing Issues;

(i) the exit criteria for testing to complete successfully;

(j) any perceived risks associated with the approach to testing and the proposed mitigations;

(k) the approach to providing for assurance of the testing undertaken; and

(l) matters to be included in the ECoS SEC Release Testing Completion Report (to be prepared pursuant to Clause 4.1).

3.3 The DCC shall submit the draft ECoS Testing Approach Document to the TAG for review (and such submission by the DCC and review by the TAG may take place prior to this Clause 3.3 coming into effect); and:

(a) where the TAG and the DCC can reach an agreement, the relevant draft ECoS Testing Approach Document shall be updated by the DCC as necessary and deemed to be final; or

(b) where the TAG and the DCC cannot reach an agreement on the approach to testing for the ECoS Variations, the matters of disagreement shall be referred by the DCC to the Secretary of State for determination. The Secretary of State's decision on such matters shall be final and binding for the purposes of this Code and the relevant draft ECoS Testing Approach Document shall be updated by the DCC as necessary and deemed to be final.

3.4 The DCC shall comply with the ECoS Testing Approach Document and shall take all reasonable steps to complete the tests set out in the ECoS Testing Approach

Document in accordance with the milestone plan published by the DCC for the ECoS Variations.

3.5 Revisions to the ECoS Testing Approach Document finalised pursuant to Clause 3.2 may, from time to time, be submitted by the DCC to the TAG for agreement in accordance with the provisions of Clause 3.3, and the provisions of Clause
3.4 shall apply (again) to the revised version of the document.

3.6 The ECoS Testing Approach Document shall set out the Devices to be used for testing. Where there is a disagreement between DCC and the TAG on Devices to be used for testing in respect of the ECoS changes, it shall be referred to the Secretary of State for determination whose decision shall be final and binding.

3.7 Where the DCC considers that User Testing is required prior to implementation of the ECoS Variations it shall set out its proposals for User Testing in a draft ECoS Mandated User Testing Document, including those Users that should be required to participate in the testing and the User Role in which they are required to participate; the approach to testing; the arrangements for test completion; the process for resolving testing disputes; and notification of test completion. In developing the ECoS Mandated User Testing Document, the DCC shall consult with the TAG, Parties, and other relevant stakeholders prior to the submission of the document to the Secretary of State.

3.8 Following consultation under Clause 3.7, the DCC shall submit the draft ECoS Mandated User Testing Document to the Secretary of State, indicating:

(a) why the DCC considers the draft to be fit for purpose;

(b) copies of the consultation responses received; and

(c) any areas of disagreement that arose during the consultation process and that have not been resolved.

3.9 The DCC shall comply with any direction given by the Secretary of State to re-consider, re-consult, and/or re-submit the draft document.

3.10 Should an ECoS Mandated User Testing Document be approved by the Secretary of State, the DCC and each Party other than the DCC that participates in (or is required to participate in) testing, as set out in such approved document, shall comply with that ECoS Mandated User Testing Document.

3.11 Each Supplier Party shall, where and to the extent reasonably requested by the DCC, provide information to the DCC relating to whether it intends to carry out testing of its User Systems in order to verify that it will be able to successfully submit "CoS Update Security Credentials" Service Requests under the ECoS Arrangements and have them successfully processed, and if so:

(a) when it proposes to carry out those tests;

(b) detail about the specific tests that it proposes to conduct, and

(c) following completion of the tests, whether or not the tests that it carried out demonstrated that the User could submit "CoS Update Security Credentials" Service Requests under the ECoS Arrangements and have them successfully executed.

4 Test Completion

4.1 Completion of the testing for the ECoS Variations set out in the ECoS Testing Approach Document shall only complete when the Panel determines that the Exit Criteria set out in that document for that testing have been met. When the DCC considers that such completion ought to occur, the DCC shall prepare a Completion Report (which may comprise part of an ECoS SEC Release Completion Report) as provided for in the ECoS Testing Approach Document. The DCC shall:

(a) notify the Secretary of State, the Authority, the Panel, TAG and the Parties that the DCC considers that testing has been completed;

(b) provide the Authority, the Panel, TAG and the Secretary of State with copies of the Completion Report (or where one exists, the ECoS SEC Release Completion Report), and a list of the sections of such report that the DCC considers should be redacted prior to publication; and

(c) review the supporting documentation and evidence with regards to the relevant Exit Criteria with the TAG.

4.2 The Panel shall confirm the completion of testing for the ECoS changes set out in the ECoS Testing Approach Document or shall highlight where it believes the Exit Criteria have not been met.

4.3 Where the Panel confirms the completion of testing for the ECoS changes (subject to the Panel and the DCC reaching an agreement regarding resolution of any issues raised by the Panel) the Completion Report (or where one exists, the ECoS SEC Release Completion Report) shall be updated by the DCC as necessary and deemed to be final.

4.4 Where the Panel declines to confirm the completion of testing for the ECoS changes, the DCC shall update the Completion Report (or where one exists, the ECoS SEC Release Completion Report) to reflect resolution of any issues where the DCC and the Panel reached an agreement, and the DCC shall then either:

(a) refer the matters where the Panel and the DCC disagree with respect to the ECoS changes to the Secretary of State for determination; or

(b) continue with testing (and Clause 4.1 onwards shall apply again).

4.5 Where a referral has been made by the DCC pursuant to Clause 4.4, the determination of the Secretary of State shall be final and binding for the purposes of this Code as follows:

(a) where the Secretary of State agrees that testing for the ECoS changes is complete, the relevant Completion Report (or where one exists, the ECoS SEC Release Completion Report) shall be updated by the DCC as necessary and the contents relating to the ECoS changes shall be deemed to be final; or

(b) where the Secretary of State disagrees that testing for the ECoS changes is complete, the DCC shall continue with testing (and Clause 4.1 onwards shall apply again).

4.6 The DCC shall publish the final Completion Report (or where one exists, the ECoS SEC Release Completion Report), which shall be anonymised and redacted where directed by the Panel, on the DCC Website. The DCC shall notify the Panel, the Secretary of State, the Authority, and the SEC Parties of the publication of the report.

Version 3.0

Appendix AS

ECoS Transition and Migration Approach Document

1 Introduction and General Obligations and Application of ETMAD

1.1 This Appendix is the ECoS Transition and Migration Approach Document (**ETMAD**).

1.2 Where directed to do so by the Secretary of State from time to time, the DCC shall develop and consult upon a further draft or drafts of this ETMAD and submit it to the Secretary of State in accordance with the process set out in Section G11.6 of the Code.

1.3 Subject to Clause 1.4, the DCC shall attempt ECoS Migration for all eligible TCoS Devices as soon as reasonably practicable. Devices shall only be eligible for ECoS Migration where they have been Commissioned (or in the case of a Gas Proxy Function has been installed as part of a Communications Hub Function that has been Commissioned) and have not subsequently been Decommissioned.

1.4 The DCC shall not attempt to migrate a particular Device that is deemed to be Ineligible for ECoS Migration. Devices may be Ineligible for ECoS Migration where:

(a) the Device is of a Device Model that has been classified as Non-Migratable;

(b) there is a transient issue which may impact the effectiveness of ECoS Migration such as recent or pending change of supplier, or recent Commissioning; or

(c) there is a technical issue impacting the functionality of the Device.

If the issue which made the Device Ineligible for ECoS Migration is subsequently resolved and / or no longer applies, the relevant Device shall no longer be Ineligible for ECoS Migration and the DCC shall attempt ECoS Migration for the Device in accordance with Clause 1.3.

1.5 The Responsible Supplier for each Device that holds Device Security Credentials that are populated from a TCoS Certificate, authorises the DCC to take the steps and carry out the processing set out in this ETMAD in order to ECoS Migrate each such Device.

1.6 The DCC shall not commence Bulk Migration for Devices of a particular Device Model until the DCC is reasonably satisfied that the DCC Systems can successfully migrate a Device of that particular Device Model in accordance with Clause 6.1(b).

1.7 Where the ECoS Migration of an individual Device is unsuccessful, the DCC shall complete remediation activities in accordance with the ECoS Migration Error Handling and Retry Approach, as further described in Clause 7.

1.8 The DCC shall issue reports to Supplier Parties in accordance with the ECoS Migration Reporting Regime, as further described in Clause 4. As a minimum these reports will contain details of:

(a) Devices that have Failed Migration; and

(b) Device Models that are categorised as Non-Migratable, together with the DCC's supporting rationale.

1.9 Responsible Suppliers shall monitor reports provided in accordance with Clause 1.8 and shall endeavour to resolve issues which led to the Failed Migration of Devices for which they are the Responsible Supplier, in accordance with the ECoS Migration Error Handling and Retry Approach.

1.10 Subject to Clause 1.11, where a Device is identified as being of a Device Model categorised as Non-Migratable or the issues leading to Failed Migrations cannot be resolved in accordance with Clause 1.9, the Responsible Supplier (except in the case of a Gas Proxy Function) shall upgrade the existing firmware version to a version of firmware that is functionally capable of ECoS Migration.

1.11 Where a Gas Proxy Function Device Model is identified as being of a Device Model categorised as Non-Migratable or the issues leading to Failed Migrations of a Gas Proxy Functions cannot be resolved in accordance with the ECoS Migration Error Handling and Retry Approach, the DCC shall be responsible for completing remediation activities with the aim of enabling ECoS Migration to proceed, including upgrading the existing firmware version to a version of firmware that is functionally capable of ECoS Migration (where applicable).

1.12 The DCC shall publish a list of Non-Migratable Device Models, to be updated regularly and as soon as practicable to reflect any changes identified.

1.13 Where a Party disagrees with the categorisation of a particular Device Model as Non-Migratable, the DCC shall endeavour to reach an agreed position with that Party. Where agreement cannot be reached, Parties may appeal the DCC's decision to categorise the Device Model as Non-Migratable to the Secretary of State.

1.14 Where an appeal has been made pursuant to Clause 1.13, the determination by the Secretary of State shall be final and binding for the purposes of this Code, provided that where a Device Model is categorised as Non-Migratable, the DCC may subsequently re-categorise the Device Model as being capable of ECoS Migration.

1.15 Supplier Parties shall take all reasonable steps to manage their inventory of Devices to prioritise the installation and Commissioning of TCoS Devices ahead of ECoS Devices. Supplier Parties shall take all reasonable steps to ensure manufacturers update their processes to initiate production of ECoS Devices as soon as reasonably practicable following receipt of the ECoS Certificate from the DCC.

1.16 The DCC shall manage the inventory of Communications Hubs to prioritise the provision of those that include Gas Proxy Functions with TCoS Certificates ahead of those with ECoS Certificates. The DCC shall take all reasonable steps to ensure providers of Communication Services update their processes to initiate production of ECoS Devices as soon as reasonably practicable following receipt of the ECoS Certificate from the DCC.

1.17 Prior to the addition of a new Device Model to the Certified Products List within the ECoS Migration Period, Supplier Parties intending to install Devices of that new Device Model shall ensure that, where reasonably practicable, testing is completed to demonstrate that ECoS Migration can be successfully performed on Devices of that Device Model, including the successful processing of a CoS Update Security Credentials Service Request (Service Reference Variant 6.23) after ECoS Migration has taken place.

1.18 The DCC shall provide updates and reports from time to time, to the Secretary of State relating to activities carried out in accordance with this ETMAD, in a format and frequency to be mutually agreed between the DCC and the Secretary of State.

1.19 Prior to the end of the ECoS Migration Period, DCC shall ensure that the ECoS Party has the required information to enable processing of CoS Update Security Credentials Service Requests (Service Reference Variant 6.23) for all SMETS1 Devices.

1.20 The ECoS Party may commence processing of CoS Update Security Credentials Service Requests (Service Reference Variant 6.23) for SMETS1 Devices at any time within the ECoS Migration Period, provided that relevant testing has been completed in accordance with the ECoS Testing Approach Document.

1.21 For the purposes of Section G11.11 of the Code, this ETMAD shall no longer apply (and shall be automatically deleted from the Code) on 1 November 2024 (or any such later date as the Secretary of State may direct following consultation on a proposed alternative with the Parties and the Panel).

2 <u>Defined Terms and Interpretation for the purposes of ETMAD</u>

Bulk Migration	means the ECoS Migration of more than a defined number of Devices of a particular Device Model. The number of Devices which constitutes Bulk Migration for a particular Device Model shall be defined by the DCC. For the avoidance of doubt, until the proving activities set out in Clause 6.1(b) have been successfully completed, no more than three hundred (300) Devices of a particular Device Model shall be migrated.
ECoS Device	means a Device which has Device Security Credentials which pertain to the ECoS Party.
ECoS Migration	has the meaning given to that term in Section G11.12 of this Code and the term

	"**ECoS Migrate**" shall be interpreted accordingly.
ECoS Migration Error Handling and Retry Approach	means the document defined in Clause 7.1.
ECoS Migration Incident	means an Incident that relates to the Services provided pursuant to this ETMAD.
ECoS Migration Period	means the period from commencement of ECoS Migration until this ETMAD is no longer applicable, in accordance with Clause 1.21.
ECoS Migration Reporting Regime	means the document defined in Clause 4.
ECoS Party	means the DCC when discharging the role of the ECoS Party.
Failed Migration	means in relation to a Device, the failure to complete any one or more of the steps specified in Clause 6.1(c).
Gas Proxy Function Device Model	means, in relation to a Gas Proxy Function, the Device Model of the Communications Hub of which that Gas Proxy Function forms part.
Ineligible for ECoS Migration	means a status applied to a Device where DCC shall not attempt ECoS Migration as further described in Clause 1.4.
Non-Migratable	(in respect of Devices of a particular Device Model) means that the DCC considers it to be (i) technically or operationally impracticable, or (ii)

	disproportionately costly to attempt or re-attempt ECoS Migration. Such determination by the DCC shall be subject to any determination to the contrary by the Secretary of State in response to an appeal as set out in Clause 1.13.
TCoS Device	means a Device which has Device Security Credentials which pertain to the TCoS Party.

2.1 For the purposes of this ETMAD, where any reference is made (either directly or indirectly) to the Device Model of a Gas Proxy Function, this shall be interpreted as a reference to the Device Model of the Communications Hub of which that Gas Proxy Function forms part.

2.2 For the purposes of this ETMAD, where any reference is made (either directly or indirectly) to the Responsible Supplier of a Gas Proxy Function, this shall be interpreted as the Responsible Supplier for the Gas Smart Meter Equipment connected to the Communications Hub, where available. Where there is no Gas Smart Meter Equipment connected to the Communications Hub, the Responsible Supplier of the Gas Proxy Function, shall be interpreted as the Responsible Supplier for the Electricity Smart Meter Equipment connected to the Communications Hub, where available. Where there is neither any Gas Smart Meter Equipment nor any Electricity Smart Meter Equipment, there will be no Responsible Supplier.

3 Transitional Application of Sections of the Code

Application of Section A (Definitions and Interpretation)

3.1 Whilst this ETMAD remains in force, Section A (Definitions and Interpretation) of the Code shall apply as follows:

(a) the definition of “DCC Individual Live Systems” (which has been replaced by the SMETS1 Transition and Migration Approach Document – Appendix AL) shall be amended to read as follows:

DCC Individual Live System

means, with regard to the DCC's duty to Separate parts of the DCC Total System, a part of the DCC Total System which is used:

(a) for one of the purposes specified in paragraphs (a) to (g) or (j) or paragraphs (l) or (m) of the definition of DCC Live Systems, where the part used for each such purpose shall be treated as an individual System distinct from:

(i) the part used for each other such purpose; and

(ii) any part used for a purpose specified in either paragraphs (h) to (k) of the definition of DCC Live Systems; or

(b) by a SMETS1 Service Provider for the purpose specified in paragraph (h) of the definition of DCC Live Systems, where the part used by each SMETS1 Service Provider shall be treated as an individual System distinct from:

(i) the part used by each other SMETS1 Service Provider; and

(ii) any part used for a purpose specified in any of paragraphs (a) to (g), or paragraphs (i) to (m), of the definition of DCC Live Systems; or

(c) by a DCO for the purpose specified in paragraph (i) of the definition of DCC Live Systems, where the part used by each DCO shall be treated as an individual System distinct from:

(i) the part used by each other DCO; and

(ii) any part used for a purpose specified in any of paragraphs (a) to (h) or paragraphs (j) to (m) of the definition of DCC Live Systems; or

(d) by a Requesting Party for the purpose specified in paragraph (k) of the definition of DCC Live Systems, where the part used by each Requesting Party shall be treated as an individual System distinct from:

(i) the part used by each other Requesting Party; and

(ii) any part used for the purpose specified in any of paragraphs (a) to (j) or paragraphs (l) or (m) of the definition of DCC Live Systems.

(b) the definition of "DCC Live Systems" (which has been replaced by the SMETS1 Transition and Migration Approach Document – Appendix AL) amended to read as follows:

DCC Live Systems means, with regard to the DCC's duty to Separate parts of the DCC Total System, those parts of the DCC Total System which are used for the purposes of:

(a) (other than to the extent to which the activities fall within paragraph (b), (c), (f), (g), (h), (i), (j), (k), (l) or (m) below) processing Service Requests, Pre-Commands, Commands, Service Responses and Alerts, holding or using Registration Data for the purposes of processing Service Requests and Signed Pre-Commands, and providing the Repository Service;

(b) Threshold Anomaly Detection (other than that carried out by a DCO, a SMETS1 Service Provider or the CoS Party) and (other than to the extent to which the activity falls within paragraph (d), (f), (g), (h), (i), (j), (k) or (l) below) Cryptographic Processing relating to the generation and use of a Message Authentication Code and Countersigning SMETS1 Service Requests;

(c) discharging the obligations placed on the DCC in its capacity as CoS Party;

(d) providing SMKI Services;

(e) the Self-Service Interface;

(f) discharging the DCC’s obligations under the SMKI Recovery Procedure; and

(g) the Production Proving Systems,

(h) discharging the obligations of any SMETS1 Service Provider in its capacity as such;

(i) discharging the obligations of any DCO in its capacity as such;

(j) discharging the obligations of the CSS Provider in its capacity as such;

(k) discharging the obligations of any Requesting Party in its capacity as such;

(l) discharging the obligations of the Commissioning Party in its capacity as such; and

(m) discharging the obligations of the TCoS Party in its capacity as such,

each of which shall be treated as an individual System within the DCC Live Systems.

(c) the definition of “Signed Pre-Command” shall be amended to read as follows:

Signed Pre-Command means a communication containing the Digitally Signed GBCS Payload of a Pre-Command that has been Digitally Signed by a User, the CoS Party or the TCoS Party.

(d) the following definitions shall be added:

TCoS Party means the DCC when discharging the role of the TCoS Party.

TCoS Systems The DCC Systems that were used to support the operation of the CoS Party immediately prior to the commencement of ECoS

Migration and that continue to be used to support the operation of the TCoS Party.

Application of Section G (Security)

3.2 Whilst this ETMAD remains in force, Section G (Security) of the Code shall be amended as follows:

(a) Clause G2.20(c) shall be replaced with the following:

‘(c) subject to the provisions of Sections G2.21 and G2.22, each DCC Individual Live System is Separated from each other such System.’

(b) Clause G2.21 shall be replaced with the following:

‘G2.21The DCC Individual Live System referred to at paragraph (m) of the definition of DCC Live Systems in Section A1 (Definitions) need not be Separated from the DCC Individual Live System referred to at paragraph (a) of that definition to the extent that it uses that System referred to at paragraph (a) solely for the purposes of confirming the relationship between:

(a) an MPAN or MPRN and any Party Details;

(b) an MPAN or MPRN and any Device; or

(c) any Party Details and any User ID.’

(c) Clause G2.44(a) amended such that the words “or TCoS Party” shall be added after the words “CoS Party”.

(d) Clause G11.12 amended such that the words “and the ETMAD” shall be added after the words “For the purposes of this Section G11”.

Application of Section H (DCC Services)

3.3 Whilst this ETMAD remains in force, Section H17.5 shall be amended to additionally include the following data items:

(a) ECoS party value;

(b) ECoS migration failure code;

(c) ECoS migration failure sub-code;

(d) ECoS migration date of last failure; and

(e) ECoS non-migratable flag.

Application of Section L (Smart Metering Key Infrastructure and DCC Key Infrastructure)

3.4 Whilst this ETMAD remains in force, Section L (Smart Metering Key Infrastructure and DCC Key Infrastructure) of the Code shall be amended as follows:

(a) In the table in Clause L3.18 the row corresponding to a Remote Party Role of 'transitionalCoS' shall be amended as follows:

transitionalCoS	The DCC	[Not applicable]	(c) or (m)

and the row corresponding to a Remote Party Role of 'coSPartyXmlSign' shall be amended as follows:

coSPartyXmlSign	The DCC	[Not Applicable]	(c) or (m)

(b) In the table in Clause L3.24 the row corresponding to a "DCC (transitionalCoS) Certificate" shall be amended as follows:

DCC (transitionalCoS) Certificate	digitalSignature	transitionalCoS	The role of the DCC as CoS Party or TCoS Party

Application of Appendix AB (Service Request Processing Document)

3.5 Whilst this ETMAD remains in force, Appendix AB (Service Request Processing Document) of the Code shall be amended as follows:

(a) Clause 6.4 shall be replaced with the following:

‘6.4 Clause 6.5 shall apply subject to:

(a) (in relation to SMETS2+ Service Requests only) Clauses 9 (Obligations of the DCC: 'Request Handover of DCC Controlled Device' Service Requests), and 11 (User and DCC Obligations: 'Join Service' and 'Unjoin' Service Requests for Pre-Payment Meter Interface Devices and Gas Smart Meters);

(b) (for all Service Requests other than SMETS1 Service Requests targeted at a TCoS Device) Clause 8 (Obligations of the DCC: 'CoS Update Security Credentials' Service Requests and (where relevant) Corresponding Pre-Commands); and

(c) (for all Service Requests) Clause 18 (Obligations of the DCC: Non-Device Service Requests).’

(b) Clause 8 shall be replaced with the following:

‘Obligations of the DCC: 'CoS Update Security Credentials' Service Requests and (where relevant) Corresponding Pre-Commands

8.1 The following shall apply in respect of each 'CoS Update Security Credentials' Service Request where the target Device of the Service Request is not a TCoS Device:

(a) where all of the requirements of Clause 6.1 are satisfied in respect of such a Service Request, the DCC shall send a Digitally Signed communication containing the ‘CoS Update Security Credentials’ Service Request (a “Countersigned CoS Service Request”) to the CoS Party; and

(b) following receipt of the Countersigned CoS Service Request , and immediately prior to creating any corresponding Update Security Credentials Signed Pre-Command referred to in Clause 8.2, the CoS Party shall:

(i) Check Cryptographic Protection for the Countersigned CoS Service Request received;

(ii) Confirm Validity of the Certificates used to Check Cryptographic Protection;

(iii) apply the checks set out in Clauses 6.1(a), 6.1(d), 6.1(e.), 6.1(f), 6.1(g), 6.1(j) and 6.1(k) to the Service Request contained within the Countersigned CoS Service Request; and

(iv) confirm that the Service Request is not a Replay.

8.1A The following shall apply in respect of each 'CoS Update Security Credentials' Service Request where the target Device of the Service Request is a TCoS Device and the Service Request is not a SMETS1 Service Request:

(a) where all of the requirements of Clause 6.1 are satisfied in respect of such a Service Request, the DCC shall send a Digitally Signed communication containing the 'CoS Update Security Credentials' Service Request (a "Countersigned CoS Service Request") to the TCoS Party; and

(b) following receipt of the Countersigned CoS Service Request specified in Clause 8.1A(a), and immediately prior to creating any corresponding Update Security Credentials Signed Pre-Command referred to in Clause 8.2A, the TCoS Party shall:

(i) Check Cryptographic Protection for both the communication and for the Service Request included within it;

(ii) Confirm Validity of the Certificates used to Check Cryptographic Protection for both the communication and for the Service Request included within it;

(iii) confirm that User ID of the User who submitted the Service Request and the User ID contained within in each of the Organisation Certificates included within the Service Request are all associated with the same User; and

(iv) confirm that the User ID in each of the Organisation Certificates included within the Service Request is that of the Party who is identified via:

(A) the relevant MPRN or MPAN (as applicable) included within the Service Request; and

(B) the Registration Data for that relevant MPRN or MPAN,

as being the Party who is (or is to be) the Responsible Supplier for the relevant Device on the specified execution date or, if the execution date is not specified, on the current date.

8.2 Where, in respect of the communication received in relation to a 'CoS Update Security Credentials' Service Request, the requirements of Clause 8.1(b) are satisfied, the CoS Party shall apply CoS Party Threshold Anomaly Detection in accordance with the requirements of Clause 20 (CoS Party Threshold Anomaly Detection), which may result in a cessation of processing of the Service Request by the CoS Party, but otherwise either;

(a) where the target Device of the original ‘Cos Update Security Credentials Service Request is a SMETS2+ Device,

(i) generate the GBCS Payload of an 'Update Security Credentials' Signed Pre-Command that is substantively identical to the 'CoS Update Security Credentials' Service Request;
(ii) Digitally Sign the GBCS Payload;
(iii) Incorporate the Digitally Signed GBCS Payload and the original Service Request into a single communication and Digitally Sign the communication with a CoS Party XML Signing Key to create a CoS Authorisation Response; and
(iv) send the signed CoS Authorisation Response to the DCC, or

(b) where the target Device of the original ‘Cos Update Security Credentials Service Request is a SMETS1 Device:

(i) Digitally Sign the communication with a CoS Party XML Signing Key to create a CoS Authorisation Response; and

(ii) send the signed CoS Authorisation Response to the DCC.

8.2A Where, in respect of the communication received in relation to a ‘CoS Update Security Credentials’ Service Request, the requirements of Clause 8.1A (b) are satisfied, the TCoS Party shall:

(a) generate the GBCS Payload of an 'Update Security Credentials' Signed Pre-Command that is substantively identical to the 'CoS Update Security Credentials' Service Request;

(b) Digitally Sign the GBCS Payload; and

(c) send the resultant communication as a Signed Pre-Command to the DCC.

8.3 Where, in respect of a communication received in relation to a 'CoS Update Security Credentials' Service Request, the requirements of Clause 8.1(b) are not satisfied:

(a) the CoS Party shall not undertake any further processing of the communication, and shall notify the DCC; and

(b) the DCC shall notify the User that sent the original Service Request that the Service Request cannot be processed (such notification to be sent via the DCC User Interface).

8.3A Where, in respect of the communication received in relation to a ‘CoS Update Security Credentials’ Service Request, the requirements of Clause 8.1A (b) are not satisfied:

(a) the TCoS Party shall not undertake any further processing of the communication and shall notify the DCC; and

(b) the DCC shall notify the User that sent the original Service Request that the Service Request cannot be processed (such notification to be sent via the DCC User Interface).

8.4 Where the DCC receives a CoS Authorisation Response from the CoS Party, the DCC shall apply the following checks:

(a) Check Cryptographic Protection for the CoS Authorisation Response;

(b) Confirm Validity of the Certificates used to Check Cryptographic Protection for the CoS Authorisation Response;

(c) Confirm that the Remote Party Role of the Certificate used to Check Cryptographic Protection for the CoS Authorisation Response is ‘coSPartyXmlSign’

(d) Confirm that the CoS Authorisation Response is valid and well formed;

(e) Confirm that the CoS Authorisation Response maps to a Countersigned CoS Service Request that was previously sent to the CoS Party;

(f) apply the checks set out in Clauses 6.1(a), 6.1(d), 6.1(e.), 6.1(f), 6.1(g), 6.1(j) and 6.1(k) to the Service Request contained within the CoS Authorisation Response;

(g) (in the circumstances where the target Device of the original ‘CoS Update Security Credentials Service Request is a SMETS2+ Device only) confirm that the Signed Pre-Command contained within the CoS Authorisation Response is substantively identical to the Service Request contained within the CoS Authorisation Response; and

(h) confirm that neither the CoS Authorisation Response, nor the Service Request contained within it is a Replay.

8.4A Where the DCC receives a Signed Pre-Command from the TCoS Party, the DCC shall apply the following checks:

(a) confirm that the User ID within each Organisation Certificate within the Signed Pre-Command is the same as the User ID within the corresponding Organisation Certificate in the original 'CoS Update Security Credentials' Service Request;

(b) confirm that the Device ID within the Signed Pre-Command is the same as the Device ID included in the corresponding 'CoS Update Security Credentials' Service Request;

(c) confirm that the message originated from the TCoS Party by Checking the Cryptographic Protection for the message;

(d) Confirm Validity of the Certificates used to Check Cryptographic Protection for the message;

(e) Confirm Validity of all Certificates contained within the Signed Pre-Command; and

(f) confirm that the User ID in each of the Organisation Certificates included within the Signed Pre-Command is that of the Party who is identified via:

(i) the relevant MPRN or MPAN (as applicable) with which the Device specified in the Signed Pre-Command is associated in the Smart Metering Inventory; and

(ii) the Registration Data for that relevant MPRN or MPAN,

as being the Party who is (or is to be) the Responsible Supplier for the relevant Device on the specified execution date or, if the execution date is not specified, on the current date.

8.5 Subject to Clause 14 (Orchestration of Service Requests), where all of the requirements of Clause 8.4 are satisfied in respect of a CoS Authorisation Response received from the CoS Party, the DCC shall:

(a) (in the circumstances where the target Device of the original ‘CoS Update Security Credentials Service Request is a SMETS2+ Device) send a Command associated with the Signed Pre-Command contained within the CoS Authorisation Response in accordance with Clause 13 (DCC Obligations: Sending Commands); or

(b) (in the circumstances where the target Device of the original ‘CoS Update Security Credentials Service Request is a SMETS1 Device) Countersign the CoS Update Security Credentials Service Request and send the Countersigned Service Request to the relevant SMETS1 Service Provider in accordance with the requirements of Clause 14.

8.5A Subject to Clause 14 (Orchestration of Service Requests), where all of the requirements of Clause 8.4A are satisfied in respect of a Signed Pre-Command received from the TCoS Party, the DCC shall send the associated Command in accordance with Clause 13 (DCC Obligations: Sending Commands).

8.6 Where any of the checks in Clause 8.4 are not satisfied in respect of a CoS Authorisation Response received from the CoS Party, the DCC shall:

(a) not be obliged to undertake any of the other checks that remain to be undertaken, and the DCC shall reject the CoS Authorisation Response;

(b) save where Clause 8.4(c) is not satisfied, notify the CoS Party of such rejection and of the reasons for such rejection; and

(c) notify the User that sent the original 'CoS Update Security Credentials' Service Request.

8.6A Where any of the checks in Clause 8.4A are not satisfied in respect of a Signed Pre- Command received from the TCoS Party, the DCC shall: not be obliged to undertake any of the other checks that remain to be undertaken, and the DCC shall reject the Signed Pre-Command;

(a) save where Clause 8.4A(c) is not satisfied, notify the TCoS Party of such rejection and of the reasons for such rejection; and

(b) notify the User that sent the original 'CoS Update Security Credentials' Service Request.’

Application of Appendix AC (Enrolment, Inventory and Decommissioning Procedures)

3.6 Whilst this ETMAD remains in force, Appendix AC (Enrolment, Inventory and Decommissioning Procedures) of the Code shall be amended as follows:

a) Clause 5.19 shall not apply; and

b) the text immediately below the table in Clause 3.2 shall be replaced with the following:

Where 'DCC Recovery Certificate', 'DCC CoS Certificate', 'DCC Access Control Broker Certificate' and 'DCC WAN Provider Certificate' are each Organisation Certificates created by the DCC for the purposes of occupying the relevant Trust Anchor Cells on Devices in accordance with the above table and used by those DCC Systems described in (respectively) sub-paragraphs (f), (c) or (m), (b) and (a) of the definition of DCC Live Systems.

Application of Appendix AG (Incident Management Policy)

3.7 Whilst this ETMAD remains in force, Appendix AG (Incident Management Policy) of the Code shall be amended as follows:

(a) the definition of Live Services (which has been replaced by the SMETS1 Transition and Migration Approach Document – Appendix AL) shall be replaced as follows:

Live Services means

(a) any of the Services that the DCC is obliged to provide to a User, an Authorised Subscriber, a DCC Gateway Party (once its connection is capable of operation), but excluding Testing Services;

(b) the exchange of data pursuant to Section E2;

(c) any of the Services provided pursuant to the TMAD; and

(d) any of the Services provided pursuant to the ETMAD

(b) Clause 2.1.3 shall not apply in respect to ECoS Migration Incidents;

(c) Clause 5.2 shall not apply in respect of DCC Systems to the extent that they are being used for ECoS Migration;

(d) where the DCC ought to be reasonably able to resolve an ECoS Migration Incident without the assistance of any Responsible Supplier, any incident resolution activities associated with an ECoS Migration Incident shall be assigned to the DCC; otherwise the incident resolution activities shall be assigned to the Responsible Supplier;

(e) the DCC shall raise an ECoS Migration Incident where monitoring of the DCC Systems identifies a problem with the DCC Systems to the extent that they are being used for ECoS Migration.

(f) the DCC shall not be required to raise an Incident, and no Party shall have the right to raise an ECoS Migration Incident, in circumstances where a Responsible Supplier is notified by the DCC in accordance with this ETMAD that one or more of the steps in the ECoS Migration of an individual Device has not been successfully completed, unless this is required by the ECoS Migration Error Handling and Retry Approach;

(g) Table 1 in Clause 2.4 shall be amended to include the following descriptions:

- Category 1 Incident: has a critical adverse impact on the activities necessary to carry out ECoS Migration pursuant to the ECoS Transition and Migration Approach Document;

- Category 2 Incident: has a non-critical adverse impact on the activities necessary to carry out ECoS Migration pursuant to the ECoS Transition and Migration Approach Document;

- Category 3 Incident: has a moderate adverse impact on the activities necessary to carry out ECoS Migration pursuant to the ECoS Transition and Migration Approach Document;

- Category 4 Incident: has a minor adverse impact on the activities necessary to carry out ECoS Migration pursuant to the ECoS Transition and Migration Approach Document;

- Category 5 Incident: has a minimal adverse impact on the activities necessary to carry out ECoS Migration pursuant to the ECoS Transition and Migration Approach Document; and

(h) Table 3 in Clause 5.2.1, row D8, column 2 shall be amended as follows: "The DCC experiences a failure of the systems used to support the operation of the CoS Party <u>or TCoS Party</u>".

<u>Application of Section M (General)</u>

3.8 The Responsible Supplier for each Device referred to in Clause 1.3 acknowledges that the carrying out of one or more of the steps referred to in this ETMAD, may result in the loss of Data stored on or in relation to each such Device and/or the ability to utilise the functionality of the Device. The DCC shall not be liable to the Responsible Supplier (or any other Party) for any Liability that arises from the carrying out of (or attempt to carry out) any of those steps, where (and to the extent that) the DCC has acted in accordance with this ETMAD.

3.9 The DCC shall carry out the activities and provide the services described in this ETMAD in accordance with Good Industry Practice. Each Responsible Supplier shall act in accordance with Good Industry Practice when providing support or assistance and carrying out remediation activities referred to in this ETMAD, in particular as set out in Clause 1.9.

3.10 Save for in respect of the Gas Proxy Function Device Model as set out in Clause 1.11 or where explicitly provided in this ETMAD, the DCC shall have no obligation or liability in respect of the ECoS Migration of any Device:

(a) With a Device Model that is categorised as Non Migratable; and / or

(b) which is deemed to be Ineligible for ECoS Migration until or unless the issue which made the Device Ineligible for ECoS Migration is subsequently resolved and / or no longer applies, such that the Device is no longer Ineligible for ECoS Migration.

4 Reporting

4.1 The DCC shall make available to the Panel, all Parties and (on request) the Secretary of State the ECoS Migration Reporting Regime that includes a list of the reports that the DCC shall provide to Supplier Parties in respect of ECoS Migration and provides an overview of the frequency, content of and recipients of those reports.

Updating the ECoS Migration Reporting Regime

4.2 Except where the modification to the ECoS Migration Reporting Regime is of a minor typographical nature or where the modification has no material effect on the rights or obligations of Parties, any updates to the ECoS Migration Reporting Regime shall be made according to the following the procedure:

(a) the DCC shall produce and publish an initial draft of the revised ECoS Migration Reporting Regime for consultation with Supplier Parties and such other persons as are likely to be interested;

(b) where a disagreement arises with any Supplier Party with regard to any proposal as to the content of the document, the DCC shall endeavour to reach an agreed proposal with that Supplier Party in accordance with this Clause 4.

(c) the DCC shall publish an updated draft of the ECoS Migration Reporting Regime as soon as is practicable after completion of the process described in (a) and (b) above together with:

(i) a statement of the reasons why the DCC considers that updated draft to be fit for purpose;

(ii) copies of the consultation responses received (apart from those marked confidential); and

(iii) a summary of any disagreements that arose during consultation that have not been resolved by reaching an agreed proposal.

4.3 Within fourteen (14) days of DCC publishing the updated draft ECoS Migration Reporting Regime pursuant to Clause 4.2(c), any Supplier Party may refer the document to the Secretary of State whose decision on its contents shall be final and binding. In the absence of any such referral, the updated draft published by the DCC shall become the agreed ECoS Migration Reporting Regime at the expiry of the fourteen (14) day period following its publication.

4.4 Where the modification to the ECoS Migration Reporting Regime is of a minor typographical nature or where the modification has no material effect on the rights or obligations of Parties, the DCC shall make the revised ECoS Migration Reporting Regime available to all Supplier Parties including providing the date on which it intends that the updated ECoS Migration Reporting Regime shall come into effect.

4.5 For each Supplier Party, the DCC shall detail directory structures in DCC's secure document management and storage system through which that Supplier Party can access its reports. The DCC shall provide a Supplier Party with only those files which are relevant to that Supplier Party and the DCC shall do so through the secure document management and storage system (which, at the time of drafting of this ETMAD is DCC's Microsoft SharePoint).

5 <u>Provision of Information to the DCC</u>

5.1 Each Supplier Party shall, on request from the DCC and within such reasonable time period as the DCC may specify, provide such information as may be reasonably required by the DCC to enable it to plan, co-ordinate, and undertake (and provide ongoing support for) ECoS Migration.

6 Migration Approach

6.1 The DCC shall determine:

(a) the process for selecting Devices for ECoS Migration, taking into account the Device Models and any exclusions as set out in Clause 1.4;

(b) the process for initiating ECoS Migration in a controlled and managed way, on the basis that, as a minimum, the DCC shall not commence Bulk Migration for Devices of a particular Device Model until it has first:

(i) successfully replaced the TCoS Certificate with an ECoS Certificate or a different TCoS Certificate on; and

(ii) subsequently demonstrated that a CoS Update Security Credentials Service Request (Service Reference Variant 6.23) has been successfully processed by,

a Device of that Device Model or a Device Model to which it can be upgraded by a firmware upgrade as set out in more detail in Clause 6.2, where activities referenced in 6.1(b)(i) and (ii) may have occurred prior to this version of the ETMAD becoming effective;

(c) the steps required to successfully complete ECoS Migration for an individual Device, including:

(i) the instruction to the TCoS Service Provider to initiate ECoS Migration;

(ii) review by the TCoS Service Provider to confirm that ECoS Migration can commence;

(iii) replacement of the Device Security Credentials that pertain to the TCoS Party with those that pertain to the ECoS Party on the relevant Device; and

(iv) confirmation received from both the ECoS Service Provider and TCoS Service Provider that ECoS Migration has completed successfully.

(d) the process for managing Failed Migrations, including the suspension of ECoS

Migration for certain Device Models to allow issues to be investigated and prevent ECoS Migration of Devices categorised as Non-Migratable; and

(e) the process for determining whether a Device Model should be categorised as Non-Migratable, subject to Clause 1.14.

6.2 For avoidance of doubt, Clause 6.1(b) allows DCC to commence Bulk Migration of Devices of a particular Device Model where the requirements set out at Clause 6.1(b)(i) and (ii) have been met for at least one Device of either (a) the same Device Model or (b) a Device Model with the same Manufacturer, same model and same hardware version but with a later firmware version, on the basis that, if ECoS Migration fails for any such Devices, the firmware version can be upgraded to a firmware version capable of ECoS Migration.

7 Error Handling and Retry Approach

7.1 The DCC shall make available to the Panel, all Parties and (on request) the Secretary of State the ECoS Migration Error Handling and Retry Approach that details the activities the DCC shall carry out where an ECoS Migration attempt is unsuccessful and the resolution activities the Supplier Party shall carry out in relation to Failed Migrations.

Updating the ECoS Migration Error Handling and Retry Approach

7.2 Except where the modification to the ECoS Migration Error Handling and Retry Approach is of a minor typographical nature or where the modification has no material effect on the rights or obligations of Parties, any updates to the ECoS Migration Error Handling and Retry Approach shall be made according to the following the procedure:

(a) the DCC shall produce and publish an initial draft of the revised ECoS Migration Error Handling and Retry Approach for consultation with Supplier Parties and such other persons as are likely to be interested;

(b) where a disagreement arises with any Supplier Party with regard to any proposal as to the content of the document, the DCC shall endeavour to reach an agreed proposal with that Supplier Party in accordance with this Clause 7.

(c) The DCC shall publish an updated draft of the ECoS Migration Error Handling and Retry Approach as soon as is practicable after completion of the process described in (a) and (b) above together with:

(i) a statement of the reasons why the DCC considers that updated draft to be fit for purpose;

(ii) copies of the consultation responses received (apart from those marked confidential); and

(iii) a summary of any disagreements that arose during consultation that have not been resolved by reaching an agreed proposal.

7.3 Within fourteen (14) days of DCC publishing the updated draft ECoS Migration Error Handling and Retry Approach pursuant to Clause 0(c), any Supplier Party may refer the document to the Secretary of State whose decision on its contents shall be final and binding. In the absence of any such referral, the updated draft published by the DCC shall become the agreed ECoS Migration Error Handling and Retry Approach at the expiry of the fourteen (14) day period following its publication.

7.4 Where the modification to the ECoS Migration Error Handling and Retry Approach is of a minor typographical nature or where the modification has no material effect on the rights or obligations of Parties, the DCC shall make the revised ECoS Migration Error Handling and Retry Approach available to all Supplier Parties including providing the date on which it intends that the updated Migration Error Handling and Retry Approach shall come into effect.

Version AT 2.0

Appendix AT

SMETS1 Cryptographic Key Management Policy for DLMS Devices

1. Introduction

This document constitutes the SMETS1 Cryptographic Key Management Policy for symmetric keys required to communicate with SMETS1 DLMS devices. The scope of the document covers DLMS devices which form part of the SMETS1 IOC and FOC cohorts.

The SMETS1 MOC cohort is not in scope of this policy as it utilises cryptographic controls provided by a S1SP Public Key Infrastructure (PKI) which falls under the governance of a S1SPKI Certificate Policy and S1SPKI Certification Practice Statement and is subject to TScheme certification and SMKI PMA approval.

Details relating to the cohort specific technical implementation of this policy are detailed in the SMETS1 Security Architecture Document and in each of the cohorts S1SP technical designs. The SMETS1 Security Architecture Document is controlled by the SEC Security Sub Committee (SSC).

DCC shall ensure that Symmetric Keys used in relation to communications with SMETS1 DLMS devices are managed and used in accordance with the requirements of this SMETS1 Cryptographic Key Management Policy.

The assurance of this policy forms a subset of the overarching security requirements defined in SEC Section G for the protection of Total System S1SP's and therefore is subject to the same level of assurance to DCC, SMKI PMA and SSC.

2. Requirement

The SEC requires in L14.7 that the DCC shall, in respect of each SMETS1 Symmetric Key Arrangement, develop a draft of a SMETS1 Cryptographic Key Management Policy, which shall:

(a) be in accordance with the requirements of "A10.1.2 – Key Management" of ISO 27001;

(b) set out the policy on the use, protection and duration of the Symmetric Keys throughout their entire lifecycle;

(c) make provision for managing those Symmetric Keys throughout their entire lifecycle, including in particular provision for generating, storing, archiving, distributing, retiring and destroying them;

(d) specify secure procedures and methods for:

i. generating Symmetric Keys for different cryptographic systems and different applications;
ii. distributing Symmetric Keys to intended recipients;
iii. activating the Symmetric Keys when received;
iv. storing Symmetric Keys and providing access to them for authorised users;
v. changing or updating Symmetric Keys, including provision for how and when they will be changed or updated;
vi. dealing with Compromised Symmetric Keys;
vii. revoking Symmetric Keys, including provision for how and when they are to be withdrawn or deactivated;
viii. recovering Symmetric Keys that are lost or corrupted;
ix. backing-up or archiving Symmetric Keys;
x. destroying Symmetric Keys; and
xi. the logging and auditing of key management related activities.

(a) be in accordance with the requirements of "A10.1.2 – Key Management" of ISO 27001;

This policy is in line with ISO 27001 A10.1.2 – Key Management which states:

A.10 Cryptography

A.10.1 Cryptographic controls

Objective: To ensure proper and effective use of cryptography to protect the confidentiality, authenticity and/or integrity of information.

A.10.1.1 A Policy on the use of cryptographic controls for protection of information shall be developed and implemented.

A.10.1.2 Key management: A policy on the use, protection and lifetime of cryptographic keys shall be developed and implemented through their whole lifecycle.

(b) set out the policy on the use, protection and duration of the Symmetric Keys throughout their entire lifecycle;

(b)(i) Use:

This document constitutes the SMETS1 Cryptographic Key Management Policy for SMETS1 DLMS devices.

DLMS meter types use four symmetric keys to send and receive instructions:

- Master Key (MK):
- Global Unicast Encryption Key (GUEK);
- Authentication Key (AK);
- Dedicated Key (DK)

SMETS1 DLMS devices have 5 separate 'clients' on the meter, these have defined roles:

- Public, used for unauthenticated access to non-sensitive information;
- Data Collection, a read-only interface to collect data from the meter;
- Extended Data Collection, a further interface to collect data from the meter;
- Management, used to make changes to the meter’s configuration; and
- Firmware, used to update the firmware of the meter.

Each of these clients (except Public) on each SMETS1 DLMS Device must have separate AK and GUEK keys unique to the meter and each client associated with it.

The term 'packaged key' is used for a key that is in a format for storage by the S1SP and use by the DCO and/or S1SP, these will be encrypted using a HSM stored Key Encryption Key.

The following symmetric key types and their uses are defined in this policy for use in SMETS1;

- Master Key (MK): the 'master' or 'key encryption' key for a single DLMS meter. Each SMTES1 DLMS device will have a Master Key (MK) that is used for key rotation.
- Global Unicast Encryption Key (GUEK): the encryption key for a single DLMS client on a single DLMS meter.

- Authentication Key (AK): the authentication key for a single DLMS client on a single DLMS meter.
- Dedicated Key (DK): the 'dedicated' or 'session' encryption key for an authenticated DLMS meter interaction.
- HSM Key: This is a Key Encryption Key stored inside a HSM for the encryption and decryption of symmetric DLMS meter keys stored by S1SPs outside of an HSM. There are two types of HSM Key Encryption Key defined in the SMETS1 Security Architecture:
- DCO Key: a HSM Key Encryption Key only stored in DCO HSM's and used to encrypt MKs and AKs stored at S1SPs.
- Shared Key: a HSM Key Encryption Key stored by both the DCO and S1SP in HSMs. Used to encrypt and decrypt GUEKs and DKs

Each SMETS1 S1SP shall only have access to the GUEK and (if used) DK.

For each command the DCO shall be provided by the S1SP the device specific AK, which must be stored by the S1SP in a packaged form where a DCO Key has been used to encrypt the AK.

In addition, for each command the DCO shall also be provided by the S1SP the GUEK and DK (if used) as required to perform cryptographic operations at the DCO.

(b)(ii) Protection & Cryptographic Processing

The DCC shall ensure that for Cryptographic Processing performed, that:

- is carried out by a SMETS1 Service Provider and involves the use of SMETS1 Global Unicast Encryption Key (GUEK); and
- after Post Migration Key Rotation has completed, is carried out by a DCO and involves the use of a packaged SMETS1 Authentication Key (AK);

Is, in each case, carried out within Cryptographic Modules that are compliant with FIPS 140-2 Level 3 (or any equivalent to that Federal Information Processing Standard which updates or replaces it from time to time).

The following encryption schemes must be used:

Symmetric Keys used for SMETS1 Device communication:

- AES_GCM 128 must be used for MKs and AKs
- AES_GCM 128 must be used for GUEKs;

Symmetric keys used for packaging MKs, AKs and GUEKs at the S1SP

- AES_ECB 128 must be used for DCO HSM Keys
- AES_ECB 128 must be used for Shared Keys.

All SMETS1 systems that generate, handle, store or distribute symmetric keys must be protected in line with SEC Section G security controls and assurance requirements.

b(iii) SMETS1 Symmetric Key Lifetime

As soon as reasonably practicable (and in any event within 7 days subject to device connectivity) following the Commissioning of a SMETS1 Communications Hub Function or a SMETS1 Smart Meter or a SMETS1 Gas Proxy Function the S1SP shall, via the DCO, in relation to each such Device and where supported by that Device, re-generate and replace any Authentication Keys and any Encryption Keys held by that Device.

Authentication Keys and any Encryption Keys generated via the DCO, following device commissioning do not subsequently need to be periodically re-generated and replaced during the life of the device. The DCC shall ensure the keys are re-generated and replaced where it is instructed to do so by the SMKI PMA in the following situations;

- As instructed in order to recover from a Major Incident where a compromise of the DCO or S1SP has occurred. PMA will consider as part of this process the need and impact of rotating symmetric keys at the DCO and/or the S1SP.
- If, as part of periodic risk and assurance reviews of the Section G controls at the DCO and S1SPs, relating to the handling of symmetric keys, these controls fall short of the minimum DCC require and where material risks are introduced that would require the re-generation and replacement of device, S1SP and DCO managed symmetric keys.

DCC must complete periodic risk reviews, at no more than 5 year intervals, of all symmetric key use and controls at the DCO and S1SPs, and provide evidence and assurance to SMKI PMA on the continued effectiveness of those controls.

(c) make provision for managing those Symmetric Keys throughout their entire lifecycle, including in particular provision for generating, storing, archiving, distributing, retiring and destroying them;

This policy makes provision for managing Symmetric Keys throughout their entire lifecycle as outlined below in Section (d).

(d) specify secure procedures and methods for:

(i) generating Symmetric Keys for different cryptographic systems and different applications;

Keys must be generated in line with each cohort's S1SP solution and in accordance with Clause 20.1 of SEC Appendix AM (SMETS1 Supporting Requirements) which states that as soon as reasonably practicable (and in any event within 7 days subject to devices connectivity) following the Commissioning of a SMETS1 Communications Hub Function or a SMETS1 Smart Meter or a SMETS1 Gas Proxy Function or a SMETS1 PPMID, the S1SP shall, via the DCO, in relation to each such Device and where supported by that Device, re-generate and replace any Authentication Keys and any Encryption Keys held by that Device.

Symmetric Keys will be automatically requested by each S1SP from the DCO as part of the Device commissioning process, where in relation to each such Device and where supported by that Device, the DCO will generate new Authentication Keys and Encryption Keys for each device DLMS client, with all cryptographic processing being carried out in Cryptographic Modules which are compliant with FIPS 140-2 Level 3 (or any equivalent to that Federal Information Processing Standard which updates or replaces it from time to time).

(ii) distributing Symmetric Keys to intended recipients;

Where supported by that Device each Device will have a Master Key (MK) that is used for key rotation and distribution. When AK and GUEK rotation is required as part of the SMETS1 commissioning obligations, the S1SP and DCO will, where supported by that Device, re-generate and replace any Authentication Keys and any Encryption Keys held by that Device and create a new Key value.

Where supported by that Device the Master Key will be rotated. Details relating to the cohort specific technical implementation of this rotation policy are detailed in the SMETS1 Security Architecture Document and in each of the cohorts S1SP technical designs and security management plans.

In the case of DCO and Shared HSM Key Encryption Keys, where the intended recipient is the DCO or the S1SP, keys will be distributed using appropriate secure transport mechanisms and digital signatures to sign the key packages to ensure the integrity and authentication of the symmetric key material as defined in the security architecture and agreed with the SMKI PMA.

(iii) activating the Symmetric Keys when received;

Where the S1SP, via the DCO, in relation to each such Device and, where supported, by that Device, re-generates and replaces any Authentication Keys and any Encryption Keys held by that Device, all such Symmetric Keys will be considered to be activated immediately.

(iv) storing Symmetric Keys and providing access to them for authorised users;

SMETS1 Symmetric Keys must be stored in compliance with SEC Section G security controls and with all cryptographic processing being carried out within Cryptographic Modules which are compliant with FIPS 140-2 Level 3 (or any equivalent to that Federal Information Processing Standard which updates or replaces it from time to time).

Access to any packed keys must be limited to S1SP Privileged Persons and only for support reasons.

All keys stored in HSMs shall be subject to controls where access is restricted to nominated ACS card holders only.

(v) changing or updating Symmetric Keys, including provision for how and when they will be changed or updated;

Authentication Keys and any Encryption Keys generated via the DCO, where supported by that Device following device commissioning, do not need to be periodically re-generated and replaced during the life of the Device other than as set out under **(b)(iii) SMETS1 Symmetric Key Lifetime** and they will not be changed or updated other than as set out in that section.

(vi) dealing with Compromised Symmetric Keys;

This policy only considers the compromise of SMETS1 Symmetric Keys held at the DCO and S1SP

In accordance with that set out under **(b)(iii) SMETS1 Symmetric Key Lifetime** of this policy, SMKI PMA may consider the need and impact of rotating one or more SMETS1 Symmetric Keys at the DCO and/or the S1SP.

(vii) revoking Symmetric Keys, including provision for how and when they are to be withdrawn or deactivated;

The SMETS1 Security architecture and DLMS Devices do not support the capability to revoke symmetric keys.

(viii) recovering Symmetric Keys that are lost or corrupted;

Should any of a Devices DLMS symmetric keys be corrupted or compromised, the S1SP and DCO will, where supported by that Device, re-generate and replace any Authentication Keys and any Encryption Keys held by that Device and create a new Key value.

(ix) backing-up or archiving Symmetric Keys;

As laid out in (viii) there is no requirement to backup or archive Symmetric Keys

(x) destroying Symmetric Keys;

The SMETS1 Security Architecture and DLMS Devices do not support the capability to destroy symmetric keys. Instead, the S1SP and DCO will, where supported by that Device, re-generate and replace any Authentication Keys and any Encryption Keys held by that Device and create a new Key value.

(xi) the logging and auditing of key management related activities

The S1SP and DCO systems and infrastructure that process SMETS1 DLMS symmetric keys form part of the wider DCC Total System and are therefore subject to the same obligations relating to Monitoring and Audit as outlined in **SEC Section G Monitoring and Audit (G2.26-G2.30).**

There are two types of logs generated as part of Symmetric key management activities:

- Environment and Infrastructure logs e.g. HSM and ACS access logs, which are subject to protective monitoring requirements.
- Logs generated during application transaction activities (e.g. all actions which involve interaction between DCO, S1SPs and devices for the creation or processing of symmetric keys)

Details relating to the cohort specific technical implementation of this policy are detailed in the SMETS1 Security Architecture Document and in each of the cohorts S1SP technical designs and security management plans.

Defined terms for the purposes of this SMETS1 Cryptographic Key Management Policy

Defined Term	Definition
Administrative Card Set (ACS)	Through smart card sets, security teams establish quorums, or a minimum number of cards that are required to perform a specific task on an HSM. There are two categories of smart card sets in HSM use: an ACS, which is used to authorise administrative tasks and disaster recovery, and one or more Operator Card Sets (OCS), which authorise HSMs to use specific application keys.
AES ECB	Advanced Encryption Standard (AES) Electronic codebook (ECB) is a block cipher mode of operation and is used for efficiency and speed for the packaging of symmetric keys.
AES GCM	Advanced Encryption Standard (AES) Galois/Counter Mode (GCM) is a mode of operation for symmetric-key cryptographic block ciphers which is widely adopted for its performance. AES-GCM is included in the NSA Suite B Cryptography as included in the DLMS specification.
Authentication Key (AK)	An authentication key for a single DLMS client on a SMETS1 Device.
DCO Key	DCO Key: a HSM Key Encryption Key only stored in DCO HSM's and used to encrypt MKs and AKs stored at S1SPs.
Dedicated Key (DK)	A 'dedicated' or 'session' encryption key for an authenticated DLMS meter interaction. Similar to an ephemeral TLS symmetric session key.
DLMS	Device Langue Message Specification. DLMS/COSEM (IEC 62056, EN13757-1) is the global standard for energy & water smart management, advanced control and innovative metering.
Final Operating Capability (FOC)	has the meaning set out in DCC's delivery plan for SMETS1 services produced pursuant to condition 13 of the DCC Licence.
Gamma	Means the secure communications network supported by Gamma Telecom Limited acting as a DCC Service Provider, or any such replacement network.
Global Unicast Encryption Key (GUEK)	An encryption key for a single DLMS client on a single SMETS1 Device.
Hardware Security Module (HSM)	means a Cryptographic Module.
HSM Key	This is a Key Encryption Key stored inside a HSM for the encryption and decryption of symmetric DLMS meter keys stored by S1SPs outside of an HSM. There are two types of HSM Key Encryption Key defined in the SMETS1 Security Architecture. DCO and Shared Keys.
Initial Operating Capability (IOC)	has the meaning set out in DCC's delivery plan for SMETS1 services produced pursuant to condition 13 of the DCC Licence.
Master Key (MK).	An encryption key that is unique to a single SMETS1 Device and that is used for key rotation.
Middle Operating Capability (MOC)	has the meaning set out in DCC's delivery plan for SMETS1 services produced pursuant to condition 13 of the DCC Licence.
Packaged Key	The term 'packaged' is used for a key that is in a format for storage by the S1SP and use by the DCO and/or S1SP, these will be encrypted using a HSM key.
Shared Key.	a HSM Key Encryption Key stored by both the DCO and S1SP in HSMs. Used to encrypt and decrypt GUEKs and DKs.
SMETS1 DLMS Device	A SMETS1 Device that uses DLMS and AES GCM Authenticated encryption. a SMETS1 Communications Hub Function or a SMETS1 Smart Meter or a SMETS1 Gas Proxy Function.

Wrapped Key	The term 'wrapped key' means a new key wrapped using the meter master key for transmission to the meter during key rotation via DLMS

Version 1.0

APPENDIX AU

Network Evolution Transition and Migration Approach Document

1. Introduction and General Obligations

1.1. This Appendix is the Network Evolution Transition and Migration Approach Document (NETMAD) developed by the DCC pursuant to Section F13 (Network Evolution Transition and Migration Approach Document) of the Code.

1.2. Where directed to do so by the Secretary of State from time to time, the DCC shall develop and consult upon a further draft or drafts of this NETMAD in accordance with Section F13.5 of the Code, and the DCC shall submit such further draft(s) to the Secretary of State in accordance with the process set out in Section F13.4 of the Code.

1.3. For the purposes of Section F13.8 (Expiry of the Network Evolution Transition and Migration Approach Document), this NETMAD will cease to apply on 30 June 2026 (or any such later date as the Secretary of State may direct following a consultation on a proposed alternative with the Parties and the Panel) and shall no longer have any effect from such date (but without prejudice to the rights and obligations arising prior to that date).

2. Defined Terms and Interpretation for the purpose of the NETMAD

2.1. The following definitions shall apply in the NETMAD:

Term	Meaning
4G Communications Hub	means a SMETS2+ Communications Hub that is designed to work with 4G mobile communications technology
4G SM WAN	means that part of the SM WAN that will utilise 4G mobile communications technology.
Carton	means a package of 14 4G Communication Hubs in a cardboard box.
Completion Report	means the completion report for Initial Pallet Validation to be completed pursuant to Clauses 4.9 – 4.14.
Initial Pallet Validation (or **IPV**)	means the initial trialling of 4G Communications Hubs by Supplier Parties in premises.
Initial Pallet Validation Approach Document	means a document produced pursuant to Clause 4.4 of this NETMAD

Term	Meaning
Initial Pallet Validation Stage	means the period during which Initial Pallet Validation will be conducted.
JIP Milestone	means a milestone within the Joint Industry Plan.
Joint Industry Plan (JIP)	means the part of the joint industry plan that relates to the 4G Communications Hubs and Network Programme that is agreed at the Department for Energy, Security and Net Zero's smart metering design group.
DCC's Microsoft SharePoint	means a web-based collaborative platform that DCC uses to securely share and exchange information with individual Parties.

2.2. Additionally, where defined terms from specific parts of the Code are used, the relevant part of the Code is stated. Where no specific part of the Code is stated, a defined term shall have its Section A (Definitions and Interpretation) meaning.

3. <u>Coverage Checker</u>

3.1. Prior to the "LSC: Go-Live decision" JIP Milestone being met, the DCC shall make available to each Supplier Party through the DCC's Microsoft SharePoint a searchable database with the capability to interrogate by post code and postal outcode whether a 4G Communications Hub installed in a premises at any given location:

(a) is expected to be able to connect to the 4G SM WAN from the start of the Initial Pallet Validation stage; or

(b) cannot be confirmed as being expected to be able to connect to the 4G SM WAN from the start of the Initial Pallet Validation stage.

3.2. The database provided pursuant to Clause 3.1 shall be a CSV file which is searchable by users at postcode and outcode level and shall be kept up to date. Whenever the DCC makes available an updated version of the database it shall notify each Supplier Party that it has done so.

4. <u>Initial Pallet Validation</u>

4.1. A Supplier Party shall not enrol a Smart Metering System incorporating a 4G

Communications Hub prior to the commencement of the Initial Pallet Validation Stage.

4.2. Each Supplier Party shall provide any information that the DCC reasonably requests in order to support the planning, coordination and undertaking of Initial Pallet Validation.

Initial Pallet Validation Approach Document

4.3. The DCC shall produce an Initial Pallet Validation Approach Document in accordance with Clause 4.4 which shall include the following:

(a) the entry criteria that are required to be met before the Initial Pallet Validation Stage can commence;

(b) the process for resolving Incidents occurring in respect of Services pertaining to the 4G mobile communications technology during the Initial Pallet Validation Stage, the applicable Incident thresholds that must not be exceeded in order for the Initial Pallet Validation Stage to complete successfully, and the process for excluding Incidents from counting towards those thresholds;

(c) the other exit criteria that are required to be met in order for the Initial Pallet Validation Stage to successfully complete, including the minimum activity that must be undertaken before the Initial Pallet Validation Stage can complete; and

(d) matters to be included in the completion report for the Initial Pallet Validation Stage.

4.4. The DCC shall submit a draft Initial Pallet Validation Approach Document to the Panel for review as soon as reasonably practicable (and such submission by the DCC and review by the Panel may take place prior to this Clause 4.4 coming into effect); and:

(a) where the Panel and the DCC can reach an agreement, the draft Initial Pallet Validation Approach Document shall be updated by the DCC as necessary and deemed to be final; or

(b) where the Panel and the DCC cannot reach an agreement, the matters of disagreement shall be referred by the DCC to the Secretary of State for determination. The Secretary of State’s decision on such matters shall be final and binding for the purposes of this Code and the draft Initial Pallet Validation

Approach Document shall be updated by the DCC as necessary and deemed to be final.

4.5. Revisions to the Initial Pallet Validation Approach Document finalised pursuant to Clause 4.4:

(a) may, from time to time, be submitted by the DCC to the SEC Panel in accordance with the provisions of Clause 4.4, and the provisions of Clause 4.4 shall apply (again) to the revised version of the document; or

(b) shall be made by the DCC in accordance with any direction to do so issued by the Secretary of State. The DCC shall consult with the SEC Panel concerning any such proposed revision in accordance with any direction to do so issued by the Secretary of State.

4.6. The DCC shall comply with the Initial Pallet Validation Approach Document.

Start of Initial Pallet Validation

4.7. Initial Pallet Validation shall only commence once the Panel has determined that the Initial Pallet Validation entry criteria have been met.

Completion of Initial Pallet Validation

4.8. Initial Pallet Validation shall only complete once the Panel has determined that the exit criteria for completion as set out in the Initial Pallet Validation Approach Document have been met.

4.9. When the DCC considers that Initial Pallet Validation completion ought to occur, the DCC shall prepare a Completion Report. The DCC shall:

(a) notify the Secretary of State, the Authority, the Panel, and the Parties that the DCC considers that Initial Pallet Validation has completed;

(b) provide the Authority, the Panel, and the Secretary of State with copies of the Completion Report and a list of the sections of such report that the DCC considers should be redacted prior to publication; and

(c) review the supporting documentation and evidence with regards to the relevant exit criteria with the Panel.

4.10. The Panel shall confirm the completion of Initial Pallet Validation or shall highlight where it believes the exit criteria have not been met.

4.11. Where the Panel confirms the completion of Initial Pallet Validation (subject to the Panel and the DCC reaching an agreement regarding resolution of any issues raised by the Panel) the Completion Report shall be updated by the DCC as necessary and deemed to be final.

4.12. Where the Panel declines to confirm the completion of Initial Pallet Validation, the DCC shall update the relevant Completion Report to reflect resolution of any issues where the DCC and the Panel reached an agreement, and the DCC shall then either:

(a) refer the matters where the Panel and the DCC are in disagreement to the Secretary of State for determination; or

(b) continue with the Initial Pallet Validation Stage (and Clause 4.9 shall apply again).

4.13. Where a referral has been made by the DCC pursuant to Clause 4.12, the determination of the Secretary of State shall be final and binding for the purposes of this Code as follows:

(a) where the Secretary of State agrees that Initial Pallet Validation has completed, the relevant Completion Report shall be updated by the DCC as necessary and the contents shall be deemed to be final; or

(b) where the Secretary of State disagrees that Initial Pallet Validation has completed, the DCC shall continue with the Initial Pallet Validation Stage (and Clause 4.8 onwards shall apply again).

4.14. The DCC shall publish the final Completion Reports for Initial Pallet Validation as soon as reasonably practicable on the DCC Website, which shall be anonymised and redacted where directed by the Panel. The DCC shall notify the Panel, the Secretary of State, the Authority and the Parties of the publication of the report.

5. <u>Ordering of 4G Communications Hubs for Initial Pallet Validation</u>

5.1. Each Supplier Party shall be entitled to order 4G Communications Hubs intended for use in the Initial Pallet Validation Stage in accordance with this Clause 5.

5.2. 4G Communications Hubs orders shall be supplied by the DCC in Cartons. Each Supplier Party may place a request for a minimum order of 1 Carton and a maximum order of 64 Cartons during the calendar month prior to the "Initial Pallet Orders" JIP Milestone. The DCC shall ensure that there are in total 640 Cartons (8,960 4G Communication Hubs) available for ordering by Supplier Parties.

5.3. The DCC shall make available to Supplier Parties at least one DCC contact telephone number and one DCC email address for the purposes of order requests for 4G Communications Hubs. A Supplier Party shall place any order request in writing by email by completing a template provided by the DCC for this purpose.

5.4. The template provided by the DCC pursuant to Clause 5.3 shall include :

(a) the number of Cartons of 4G Communications Hubs being ordered (which, in accordance with Clause 5.2, shall be between 1 and 64 Cartons);

(b) one Delivery Location for the order, including the following information for the Delivery Location:

(i) the full delivery address (including postcode);

(ii) days of the week and hours within those days that deliveries can be made;

(iii) a preferred delivery date within one month preceding the “Initial Pallet Supply” JIP Milestone; and

(iv) the name, email address, and telephone number for a nominated contact in relation to each Communications Hubs order.

5.5. Where a Supplier Party does not provide an order request in a number of Cartons or where the order request is more than 64 Cartons, DCC shall amend that element of the request at its discretion to comply with the requirements set out in this Clause 5..

5.6. Where the DCC receives a Communications Hub order request from a Supplier Party, the DCC shall:

(a) promptly acknowledge receipt of the request; and

(b) within five Working Days of its receipt, notify the Supplier Party in writing via email either that:

(i) the request satisfies the requirements of Clause 5.4 and is therefore being processed; or

(ii) the request does not satisfy the requirements of Clause 5.4 with respect to the minimum or maximum number of Cartons therefore that the DCC has amended the order request pursuant to Clause 5.5, provide the details of the amendment and state that the request is being processed on that basis; and/or

(iii) the request does not satisfy the other requirements of Clause 5.4 in which case the Supplier Party shall revise the request within [5] Working Days so that it does so satisfy those requirements, in order for it to be eligible for processing by the DCC.

5.7. Following completion of the steps in Clause 5.6, the DCC shall process each Supplier Party's order request in accordance with the rules set out in Clauses 5.8 – 5.15.

5.8. Where the aggregate of the order requests pursuant to Clause 5.6 exceeds 640 Cartons, the following rules shall apply and the DCC shall adjust each Supplier Party's order request accordingly:

(a) each order request for 16 Cartons or fewer shall be accepted. Each order request for more than 16 Cartons shall be reduced by one Carton. This process shall be repeated until the aggregate number of order requests does not exceed 640 Cartons, provided that the DCC shall not reduce a Supplier Party's order request below 16 Cartons; and

(b) once the rules in Clause 5.8(a) have been applied, any remaining Cartons that are available to be ordered shall be randomly allocated to individual order requests that were reduced pursuant to Clause 5.8(a).

5.9. Where the aggregate of order requests pursuant to Clause 5.6 equals 640 Cartons, no further adjustment shall be made by the DCC to each Supplier Party's order request.

5.10. Where the aggregate of order requests pursuant to Clause 5.6 is fewer than 640 Cartons, the DCC shall send an email to each Supplier Party that submitted an order request to invite them to increase their order request through an additional round of requests, stating the total amount of Cartons that are available for ordering in that additional round that have not yet been requested. Each Supplier Party shall have 5 Working Days to respond in writing via email to the DCC stating whether it wants to additionally request Cartons and if so, the number that it wishes to additionally request. Where a Supplier Party does not submit an additional order request, its order request shall not be amended.

5.11. In respect of those Supplier Parties that do submit additional order requests, where the aggregate of the additional order requests received pursuant to Clause 5.10 does not exceed the total Cartons that were available for ordering in the additional round, the DCC shall adjust each relevant Supplier Party's order request to reflect the additional amount requested by that Supplier Party.

5.12. In respect of those Supplier Parties that do submit additional order requests, where the aggregate of the additional order requests received pursuant to Clause 5.10 exceeds the total Cartons that were available for ordering in the additional round, then the following rules shall apply and the DCC shall adjust each relevant Supplier Party's order request to reflect the additional amount allocated to that Supplier Party:

(a) the DCC shall reduce the Supplier Party's additional order request by a single Carton. This process shall be repeated until the aggregate number of additional order requests does not exceed the total number of Cartons that were available for ordering in the additional round; and

(b) once the rules in Clause 5.12(a) have been applied, any remaining Cartons that are available shall be randomly allocated to individual additional order requests that were reduced pursuant to Clause 5.12(a).

5.13. In the event that a Supplier Party's order request or additional order request is amended pursuant to Clause 5.8 or Clause 5.12, the DCC shall contact that Supplier Party by email, to inform them of the amendment, setting out the reason for the change.

5.14. Each Supplier Party's accepted order for 4G Communications Hubs will be set at the amount of Cartons established pursuant to completion of the process set out in Clauses

5.8 – 5.12 (inclusive). The DCC shall notify each Supplier Party in writing via email of its accepted order amount by the "Initial Pallet Orders" JIP Milestone.

5.15. The DCC shall deliver to each Supplier Party its accepted order of 4G Communications Hubs to the location set out in the order request, within the opening hours of that location and on the delivery date established pursuant to Clause 5.4(b)(iii).

5.16. The DCC and each Supplier Party acknowledges that the DCC Licence and other parts of this Code (including Section A, Section F, the CH Handover Support Materials and the CH Installation and Maintenance Support Materials) shall be amended prior to delivery to apply in respect of the 4G Communications Hubs ordered pursuant to this Clause 5 and in respect of the Services that the DCC shall be required to provide in relation to those Communications Hubs.