

This document is classified as **White** in accordance with the Panel Information Policy. Information can be shared with the public, and any members may publish the information, subject to copyright.



DP212 'Housekeeping changes 2022'

Modification Report

Version 0.1

12 July 2022

Corporate member of
Plain English Campaign
Committed to clearer
communication

592



Managed by



About this document

This document is a draft Modification Report. It currently sets out the background, issue, and progression timetable for this modification, along with any relevant discussions. This document will be updated as this modification progresses.

Contents

1. Summary.....	3
2. Issue.....	3
3. Solution	4
4. Impacts	4
5. Costs	7
6. Implementation approach	7
7. Case for change.....	7
Appendix 1: Progression timetable	8
Appendix 2: Glossary	9

This document has one Annex:

- **Annex A** contains the redlined changes to the Smart Energy Code (SEC) required to deliver the Proposed Solution.

Contact

If you have any questions on this modification, please contact:

Elizabeth Woods

020 4566 8335

elizabeth.woods@gemserv.com

1. Summary

This proposal has been raised by Tom Rothery from the Data Communications Company (DCC).

The Smart Energy Code Administrator and Secretariat (SECAS) maintains a log of typographical errors, cosmetic and other inconsistencies, omissions and other clarifications that are required to be corrected within SEC documentation. Any such instances that are identified by any party and notified to SECAS are placed on the log and will be amended at an appropriate point. The Proposed Solution to this modification aims to address all the outstanding issues that are currently identified on the log, and any identified and notified to SECAS while the modification is in progress.

This modification will have no direct impacts on any SEC Party but will give greater clarity and transparency to the SEC Documents. There will be no DCC System costs. This is proposed to be progressed as a Fast-Track Modification and is targeted for the November 2022 SEC Release.

2. Issue

What are the current arrangements?

The current SEC Documents have some minor errors which were in the SEC from inception or introduced in via various changes over the years. SECAS maintains a log of these errors, which are either identified by SECAS or notified to SECAS by other parties. The usual process is to add these into a modification if a particular SEC Document is undergoing changes due to a modification. However, a number of these errors have been on the housekeeping log for several years due to modifications to which these had been added being rejected or no modifications making amendments to the relevant documents.

What is the issue?

Some of the errors on the housekeeping log have not been addressed despite being logged for several years. This is because either a modification which makes changes to the relevant section has never been raised or because a modification which the housekeeping changes were include in has been rejected or withdrawn, leading to the housekeeping issues not being addressed. The type of housekeeping changes included in this modification are listed below:

Minor typographical and grammatical errors

This is a compilation of minor inconsistencies found by various parties over the last few years and has been awaiting a general housekeeping modification to address.

Inconsistencies introduced by other modifications

Some inconsistencies have been introduced by the implementation of modifications. [MP138 'DCC Service Testing in ETAD'](#) introduced some new descriptions for some testing methodologies into

Section H; these did not align with existing definitions in Section A and need to be aligned to ensure consistency.

The term 'Technical Code Specifications' covers various SEC Schedules and Appendices, otherwise known as SEC Subsidiary Documents. However, the 'SSI Baseline Requirements Documents' is a code required document managed by the DCC and was included in this list in error via ['SECMP0058 Changes to the governance of the Self-Service Interface'](#).

Several instances of 'unique identifier' need to be updated to 'Market Participant Identifier' as result of the changes made by Urgent modification [MP185 'Additional controls to support the SoLR process'](#).

What is the impact this is having?

If these corrections are not resolved, the SEC Documents will contain inconsistencies. Although these are minor typographical, cosmetic and alignment inconsistencies, as well as apparent inconsistencies and omissions between different SEC documents, leaving these in could cause confusion for Parties reading these sections.

If these continue to remain, it could make it harder for Parties to comply with these documents and make the documents in question harder to maintain, increasing the chance of further inconsistencies occurring in the future.

Impact on consumers

The issue outlined in this proposal does not impact consumers.

3. Solution

Proposed Solution

The Proposed Solution is to correct the minor errors and inconsistencies identified in the SEC Documents.

The legal text can be found in Annex A.

4. Impacts

This section summarises the impacts that would arise from the implementation of this modification.

SEC Parties

SEC Party Categories impacted	
Large Suppliers	Small Suppliers

SEC Party Categories impacted			
	Electricity Network Operators		Gas Network Operators
	Other SEC Parties		DCC

All SEC Parties

There are no direct impacts from this modification. All Parties will indirectly benefit from this modification as the SEC Documents will have greater clarity and transparency.

DCC System

This modification does not impact the DCC Systems.

SEC and subsidiary documents

The following parts of the SEC will be impacted:

- Section A 'Definitions and Interpretations'
- Section C 'Governance'
- Section F 'Smart Metering System Requirements'
- Section G 'Security'
- Section H 'DCC Services'
- Section J 'Charges'
- Section K 'Charging Methodology'
- Section L 'Smart Metering Key Infrastructure and DCC Key Infrastructure'
- Section M 'General'
- Section P 'Production Proving'
- Section T 'Testing During Transition'
- Section Z 'The Alt HAN Arrangements'
- Schedule 5 'Accession Information'
- Schedule 6 'Specimen Form of Letter of Credit'
- Appendix B 'Organisation Certificate Policy'
- Appendix D 'SMKI Registration Authority Policies and Procedures'
- Appendix E 'DCC User Interface Services Schedule'
- 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 Test Approach Document'

Managed by

- Appendix L 'SMKI Recovery Procedure'
- Appendix O 'SMKI Repository Interface Design Specification'
- Appendix S 'DCCKI Certificate Policy'
- Appendix X 'Registration Data Interface Specification'
- Appendix Z 'CPL Requirements Document'
- Appendix AB 'Service Request Processing Document'
- Appendix AG 'Incident Management Policy'
- Appendix AI 'Self Service Interface Code of Connection'
- Appendix AJ 'SEC Variation Testing Approach Document'
- Appendix AL 'SMETS1 Transition and Migration Approach Document'
- Appendix AN 'SEC Variation Testing Approach Document for BEIS Changes included in the November 2020 SEC Release'
- Appendix AO 'S1SPKM Compliance Policy'
- Appendix AP 'FOC S1SPKI Certificate Policy'
- Appendix AP 'Secure S1SPKI Certificate Policy'
- Appendix AQ 'SEC Variation Testing Approach Document for the CH&N Arrangements'
- Appendix AS 'ECoS Transition and Migration Approach Document'
- Appendix AT 'SMETS1 Cryptographic Key Management Policy'

The changes to the SEC required to deliver the Proposed Solution can be found in Annex A.

Technical specification versions

Due to the approach for managing and updating technical specifications, changes to these documents have been left out of this modification. This is to mitigate the risk that no other changes to that technical specification are made in the corresponding release, resulting in a new sub-version for no material benefit.

Devices

Devices will not be impacted by this modification

Consumers

This modification does not impact consumers.

Other industry Codes

This modification does not impact any other industry Codes.

Greenhouse gas emissions

This modification does not impact greenhouse gas emissions.

5. Costs

DCC costs

There are no DCC costs associated with this modification.

SECAS costs

The estimated SECAS implementation cost to implement this as a stand-alone modification is two days of effort, amounting to approximately £1200. This cost will be reassessed when combining this modification in a scheduled SEC Release. The activities needed to be undertaken for this are:

- Updating the SEC and releasing the new version to the industry.

SEC Party costs

There are no SEC Party implementation costs associated with this modification.

6. Implementation approach

Recommended implementation approach

SECAS is recommending an implementation date of:

- **3 November 2022** (November 2022 SEC Release) if a decision to approve is received on or before 20 October 2022; or
- **23 February 2023** (February 2023 SEC Release) if a decision to approve is received after 20 October 2022 but on or before 9 February 2023.

7. Case for change

Business case

This modification will only incur the costs from SECAS time and effort and will correct inconsistencies that have been in the SEC for several years and have not been addressed yet.

Views against the General SEC Objectives

Proposer's views

The Proposer believes that the modification will better facilitate SEC Objective (a)¹ as it will correct errors in the SEC and lead to less confusion or interpretation.

Views against the consumer areas

Improved safety and reliability

The implementation of this modification will have a neutral impact on safety and reliability.

Lower bills than would otherwise be the case

The implementation of this modification will have a neutral impact on bills.

Reduced environmental damage

The implementation of this modification will have a neutral impact on reducing environmental damage.

Improved quality of service

The implementation of this modification will have a neutral impact on quality of service.

Benefits for society as a whole

The implementation of this modification will have a neutral impact on benefits for society.

Final conclusions

This modification addresses many ears of inconsistencies and points of potential confusion or misinterpretation. There are no DCC costs and only a minimum SECAS cost to implement.

Appendix 1: Progression timetable

This Draft Proposal was raised on 12 July 2022 and will be taken to the Change Sub-Committee (CSC) for initial comment on 19 July 2022. SECAS considers that this modification would meet the requirements to be a Fast-Track Modification, as the changes are all typographical errors or other minor factual inaccuracies or inconsistencies in the SEC that would not constitute material changes (SEC Section D2.8). SECAS is proposing leaving this proposal in the Development Stage for a month

¹ Facilitate the efficient provision, installation, operation and interoperability of smart metering systems at energy consumers' premises within Great Britain.

to allow Parties a chance to review and comment on the legal text, before asking the CSC to approve this as a Fast-Track Modification in August 2022.

For this to be approved as a Fast-Track Modification, the CSC decision would have to be unanimous. There would then be 15 Working Days for Parties to object to this decision, after which the CSC's approval would be final and the modification implemented. If the CSC is not unanimous or any objection is subsequently raised, this modification could not progress as Fast-Track and would have to be progressed to decision via another route.

Timetable	
Event/Action	Date
Draft Proposal raised	12 Jul 2022
Presented to CSC for initial comment	19 Jul 2022
Legal text available for industry comment	Jul-Aug 2022
CSC converts Draft Proposal to Modification Proposal	16 Aug 2022
CSC approves modification as Fast-Track Modification	16 Aug 2022
Objection period ends	7 Sep 2022

Appendix 2: Glossary

This table lists all the acronyms used in this document and the full term they are an abbreviation for.

Glossary	
Acronym	Full term
Alt HAN	Alternative Home Area Network
CPL	Central Products List
CSC	Change Sub-Committee
DCC	Data Communications Company
DUIS	DCC User Interface Specification
ECoS	Enduring Change of Supplier
ETAD	Enduring Testing Approach Document
FOC S1SPKI	Final Operating Capability SMETS1 Service Provider Public Key Infrastructure
S1SPKI	SMETS1 Service Provider Public Key Infrastructure
S1SPKM	SMETS1 Service Provider Key Management
SEC	Smart Energy Code
SECAS	The Smart Energy Code Administrator and Secretariat
SMKI	Smart Metering Key Infrastructure
SoLR	Supplier of Last Resort
SSI	Self-Service Interface

This document is classified as **White** in accordance with the Panel Information Policy. Information can be shared with the public, and any members may publish the information, subject to copyright.

DP212 ‘Housekeeping changes 2022’

Legal text – version 0.1

About this document

This document contains the redlined changes to the SEC that would be required to deliver this Modification Proposal.

Section A ‘Definitions and Interpretation’

These changes have been redlined against Section A version 24.0.

Amend Section A 1.1 as follows (housekeeping change):

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:

Interoperability and Innovation Events	means the events held by the DCC from time to time <u>and</u> at its discretion, to provide Device Manufacturers with a <u>Testing Service (referred to as Interoperability and Innovation Events) that provides a platform for Testing Participants</u> to test connectivity, interoperability, interchangeability and functionality between <u>SMETS2+ Home Area Network (HAN)</u> Devices.
RF Noise Testing	means a testing service provided by the DCC to enable <u>Testing Participants</u> Device Manufacturers to test their Devices <u>and to</u> ensure they meet the requirements of the <u>Intimate Communications Hub Interface Specification (ICHIS) published on the DCC Website in accordance with SEC Section H12</u> , so they do not impact the WAN or HAN performance.
Wired Instrumented Test Communications Hubs	means a <u>testing service (referred to as Wired ITC Provision) provided by the DCC, Test Communications Hub which enables Participants to undertake interoperability testing and message handling with a SMETS2+ Test Communications Hub across</u> is capable of sending WAN Commands through a wired interface during GFI Testing.
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 SSI Baseline Requirements Document , 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.

Section C ‘Governance’

These changes have been redlined against Section C version 8.0.

Amend Section C 1.1(g) as follows (housekeeping change):

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.

Amend Section C 4.4(a) as follows (housekeeping change):

C4. ELECTED MEMBERS

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).

Amend Section C 7.10 as follows (housekeeping change):

C7. CODE ADMINISTRATOR, SECRETARIAT AND SECCO

Code Administrator

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, and 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.

Section F 'Smart Metering System Requirements'

These changes have been redlined against Section F version 11.0.

Amend Section F2.11(a) & F11.1 as follows (housekeeping change):

F2. CENTRAL PRODUCTS LIST

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.

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**").

Section G ‘Security’

These changes have been redlined against Section G version 14.0.

Amend Section G2 as follows (housekeeping change):

G2. SYSTEM SECURITY: OBLIGATIONS ON THE DCC

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 at 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 service provider 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 G2.22~~CD~~ and G2.22~~DE~~ 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 G2.22C and G2.22D 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 G2.22~~AB~~(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 G2.22~~AB~~(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 G2.22~~AB~~(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 G2.22~~AB~~(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 G2.22 ~~DE~~(b)(i) and (ii), including any fines or re-procurement costs.

Amend Section G5 as follows (housekeeping change):

G5. INFORMATION SECURITY: OBLIGATIONS ON THE DCC AND USERS

Information Security: Obligations on Users

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.

Amend Section G7 as follows (housekeeping change):

G7. SECURITY SUB-COMMITTEE

Duties and Powers of the Security Sub-Committee

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; and
- (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.

Amend Section G8 as follows (housekeeping change):

G8. USER SECURITY ASSURANCE

Initial Full User Security Assessment: User Entry Process

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).

Section H 'DCC Services'

These changes have been redlined against Section H version 14.0.

Amend Section H1 as follows (housekeeping change):

H1. USER ENTRY PROCESS

User IDs

- 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 the combined User Roles of either, 'Import Supplier' and 'Gas Supplier' or 'Import Supplier', 'Export Supplier' and 'Gas Supplier'.

User Entry Process Requirements

- 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.

Amend Section H7 as follows (housekeeping change):

H7. USER ENTRY PROCESS

Formal Offer

- 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.

Amend Section H8 as follows (housekeeping change):

H8. SERVICE MANAGEMENT, SELF-SERVICE INTERFACE AND SERVICE DESK

Self-Service Interface

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;

Amend Section H9 as follows (housekeeping change):

H9. INCIDENT MANAGEMENT

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

H9.4 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.

Amend Section H10 as follows (housekeeping change):

H10. BUSINESS CONTINUITY

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.

Amend Section H11 as follows (housekeeping change):

H11. PARSE AND CORRELATE SOFTWARE

Provision of Parse and Correlate Software

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; ~~and~~
- (b) can be confirmed, on receipt by the person to whom it is provided:
 - ~~(e)(i)~~ as having been provided by the DCC; and
 - ~~(i)(ii)~~ as being authentic, such that any tampering with the software would be apparent.

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).

Amend Section H12 as follows (housekeeping change):

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.

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.

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.

Amend Section H13 as follows (housekeeping change):

H12. 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):

Amend Section H14 as follows (housekeeping change):

H14. TESTING SERVICES

Modification Implementation Testing

- 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.

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 ESME or a Communication Hub Hot Shoe~~ to ensure ~~they~~ it meets 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.

Interoperability and Innovation Events

- H14.49 The DCC shall, from time to time and at its discretion, provide a Testing Service (referred to as Interoperability and Innovation Events) that provides a platform for Testing Participants ~~Device Manufacturers~~ to test connectivity, interoperability, interchangeability and functionality between SMETS2+ Home Area Network (HAN) Devices.

Wired Instrumented Test Communications Hubs

- H14.54 The DCC shall provide a Testing Service (referred to as Wired ITCH Provision), ~~which~~ enables ~~Testing~~ Participants to ~~perform undertake~~ interoperability testing and message handling with a SMETS2+ Test Communications Hub across a wired interface that will facilitate the sending of DUIS Commands to HAN Devices.

Amend Section H16 as follows (housekeeping change):

H16. INTEROPERABILITY CHECKER SERVICE

The Responsibility of Supplier Parties

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.

H16.5 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

H16.7 -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.

Section J 'Charges'

These changes have been redlined against Section J version 9.0.

Amend Section J1.7 as follows (housekeeping change):

J1. PAYMENT OF CHARGES

Payment of Charges

- 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.

Section K 'Charging Methodology'

These changes have been redlined against Section K version 12.0.

Amend Section K6 as follows (housekeeping change):

K6A. DETERMINING FIXED CH CHARGES

Determining the Fixed CH Charges

~~K6A.4~~ [Not used]

Amend Section K7 as follows (housekeeping change):

K7. DETERMINING EXPLICIT CHARGES

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) 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); or (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;
- (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 F7.89 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; and
 - (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).

Explicit 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.

Amend Section K11 as follows (housekeeping change):

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:

Section L ‘Smart Metering Key Infrastructure and DCC Key Infrastructure’

These changes have been redlined against Section L version 14.0.

Amend Section L3 as follows (housekeeping change):

L3 THE SMKI SERVICES

Market Participant Identifier~~Unique 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 Identifier~~Unique 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~~Unique 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 Identifier~~~~Unique 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~~~~Unique 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~~~~Unique 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~~~~Unique 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; ~~and~~

(d) ~~“Unique Identifier” means a unique identifier by which a Supplier Party may be identified in the Party Details.~~

Section M ‘General’

These changes have been redlined against Section M version 8.0.

Amend Section M10 as follows (housekeeping change):

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).

Section P ‘Production Proving’

These changes have been redlined against Section P version 7.0.

Amend Section P1 as follows (housekeeping change):

P1. PRODUCTION PROVING

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 a Registration Data Provider in respect of Production Proving Registration Data.

Section T ‘Testing During Transition’

These changes have been redlined against Section T version 8.0.

Amend Section T5 as follows (housekeeping change):

T5. SMKI AND REPOSITORY TESTING

Completion of SMKI and Repository Testing

T5.21 On application of the DCC pursuant to Section T5.19, the Panel shall:

- (a) determine whether or not the exit criteria have been met;
- (b) notify its decision to the Secretary of State, the Authority and the Parties, giving reasons for its decision-; and
- (c) direct the DCC to publish its report, subject to the redaction of those sections of the report which the Panel considers to contain information which may pose a risk of Compromise to the DCC Total System, RDP Systems and/or User Systems (which sections may or may not include those sections which the DCC proposed for redaction).

Section Z ‘The Alt HAN Arrangements’

These changes have been redlined against Section Z version 9.0.

Amend Section Z1.22 as follows (housekeeping change):

Z1. THE ALT HAN FORUM

Proceedings of the Forum

Alternates

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 ~~is~~ Chair is unable to be available to perform his or her role, a reference to the Alternate Chair.

Amend Section Z3.1 as follows (housekeeping change):

Z3. ALT HAN SECRETARIAT

- Z3.1 ~~AltHANC~~ 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**.

Amend Annex to Section Z as follows (housekeeping change):

Annex – AltHANC

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 Section Z of this Code coming into effect, ~~at which the business set out in [ref] to this Annex was undertaken. As set out in that [ref], such business is to have effect from Section Z of this Code coming into effect.~~

3.2 The consequence of the resolutions referred to above is that, with effect from Section Z of this Code coming into effect, each of the Subscribing Shareholders is a Shareholder and each of the Board Members is a Director.

Schedule 5 'Accession Information'

These changes have been redlined against Schedule 5 version 8.0.

Amend Schedule 5 as follows (housekeeping change):

15. Where applicable, details of the unique identifiers by which the Applicant is identified ~~Applicant's status~~ as a Meter Operator or a Meter Asset Manager for an MPAN or MPRN.

Schedule 6 'Form of letter of credit'

These changes have been redlined against Schedule 6 version 7.0.

Amend Schedule 6 as follows (housekeeping change):

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 ensure 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.

Appendix B ‘Organisation Certificate Policy’

These changes have been redlined against Appendix B version 6.0.

Amend Appendix B4 as follows (housekeeping change):

4 CERTIFICATE LIFE-CYCLE OPERATIONAL REQUIREMENTS

4.1 CERTIFICATE RENEWAL

4.6.2 Circumstances of Certificate Replacement

- (i) 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 ~~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 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.
- (ii) 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.

(iii) 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.

Amend Appendix B Annex A as follows (housekeeping change):

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.

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.

Amend Appendix B Annex B as follows (housekeeping change):

ANNEX B: OCA CERTIFICATE AND ORGANISATION CERTIFICATE PROFILES

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.

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 Identifier~~unique 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 Unique Identifier

This shall be populated with the 64-bit Entity Identifier of the subject of the Certificate

Appendix D ‘SMKI Registration Authority Policies and Procedures’

These changes have been redlined against Appendix D version 4.0.

Amend Appendix D7.2 as follows (housekeeping change):

7 Submission of CSRs and Issuance of Certificates

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~~~~unique identifiers~~ 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~~~~unique 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 Identifiers~~~~unique identifiers~~ 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.

Appendix E 'DCC User Interface Services Schedule'

These changes have been redlined against Appendix E version 6.0.

Amend Appendix E as follows (housekeeping change):

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
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.
12.2	12.2	Device Pre-notification	Import Supplier, Gas Supplier, Registered Supplier Agent, Electricity Distributor, Gas Transporter , Export Supplier, Other User	30 seconds	16 seconds	✓	

Appendix G 'DCC Gateway Connection Code of Connection'

These changes have been redlined against Appendix G version 2.0.

Amend Appendix G as follows (housekeeping change):

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.

Appendix H 'CH Handover Support Materials'

These changes have been redlined against Appendix H version 2.0.

Amend Appendix H Annex C as follows (housekeeping change):

Annex C. ~~Annex C~~ Communications Hub storage and installation environmental conditions

Appendix I 'CH Installation and Maintenance Support Materials'

These changes have been redlined against Appendix I version 4.0.

Amend Appendix I as follows (housekeeping change):

Definitions

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).
-------------------------------------	--

5. COMMUNICATIONS HUB DIAGNOSTICS

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.

8. ON-SITE FAULT RESOLUTION AND COMMUNICATIONS HUB REPLACEMENT

Special Installation Mesh Communications Hub Fault Handling Procedures

- 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.

10. COMMUNICATIONS HUB RETURNS

- 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 ~~this~~ clauses 10.1 to 10.20 of this document.

Annex A. CH Fitting and removal procedures

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.2. Communications Hub Activation Procedure - Central Region and South Region

- 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'.

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 E. Equipment Supplied

E.2. Central and South Regions

- 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-~~2~~-GHz

Appendix J 'Enduring Testing Approach Document'

These changes have been redlined against Appendix J version 5.0.

Amend Appendix J5 as follows (housekeeping change):

5. Obligations on Testing Participants using Remote Test Labs

- 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.

Appendix L ‘SMKI Recovery Procedure’

These changes have been redlined against Appendix L version 5.0.

Amend Appendix L1 as follows (housekeeping change):

1. Introduction

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).

Amend Appendix L2 as follows (housekeeping change):

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).

Compromise or Suspected Compromise of:	Section(s) of this document containing the procedure(s)
Replacement of an XML Signing Private Key	7.1.1 XML Signing Private Key -destruction considerations

Amend Appendix L4 as follows (housekeeping change):

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

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

Step	When	Obligation	Responsibility	Next Step
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. 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	Subscriber	4.1.1.3

		that the Anomaly Detection Thresholds File is submitted in accordance with the provisions of the TADP.		
--	--	--	--	--

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

Step	When	Obligation	Responsibility	Next Step
4.3.1.7	As soon as reasonably practicable, following 4.3.1.6	The SMKI PMA shall: - 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; - 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 - if the SMKI PMA has determined that steps in this procedure should be undertaken, detail the actions that the Subscriber is to undertake, in 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.	SMKI PMA, DCC	4.3.1.8

Amend Appendix L5 as follows (housekeeping change):

5. Recovery using the Contingency Private Key

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
5.2.3	As soon as possible, following 5.2.2	Where: - The DCC is to issue Commands using the Contingency Private Key, the DCC shall, where necessary, amend the relevant Anomaly Detection Thresholds; and - the affected Subscriber is to submit submit Service Requests to replace DCC Access Control Broker Certificates with Organisation	DCC (DSP TAD)	5.2.4

		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 5.2.2, that the Anomaly Detection Threshold values have been successfully amended.		
--	--	--	--	--

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
5.3.2	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: - 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 - the DCC Access Control Broker Certificate in each Network 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.	Subscriber	5.3.3

Amend Appendix L6 as follows (housekeeping change):

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

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
6.1.1.3	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): - 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; - notifying Key Custodians to attend the relevant Key Generation Ceremony; and - activities required to prepare such systems environment required to support: - generation of a new Contingency Key Pair; - creating a new M#N Share of the Contingency Private Key; - generation of a new Contingency Symmetric Key; - encryption of the new Contingency Public Key using the new Contingency Symmetric Key; - for the new symmetric key, conducting Contingency Symmetric Key Splitting; - generation of a replacement Root OCA Certificate, containing the Public Key from the current Root OCA Certificate and the new encrypted Contingency Public Key;	DCC, Key Custodians	6.1.1.4

Amend Appendix L7 as follows (housekeeping change):

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.

Amend Appendix L 'Appendix G' as follows (housekeeping change):

Appendix G: SMKI Recovery Procedure Test Scenarios

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

Appendix O ‘SMKI Repository Interface Design Specification’

These changes have been redlined against Appendix O version 5.0.

Amend Appendix O1.2 as follows (housekeeping change):

1 Introduction

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.

Amend Appendix O1.2 as follows (housekeeping change):

2 Interface Definition

2.3 SSH File Transfer Protocol (SFTP) Interface

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.

Appendix S ‘DCCKI Certificate Policy’

These changes have been redlined against Appendix S version 4.0.

Amend Appendix S ‘Annex A’ as follows (housekeeping change):

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

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.
--	--

Amend Appendix S ‘Annex B’ as follows (housekeeping change):

ANNEX B

DCCKI CERTIFICATE PROFILES

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, ~~and~~ 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.

DCCKI Infrastructure Certificate DCCKI Certificate Profile for the purposes of establishing SAML assertions

Interpretation 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

Personnel Authentication Certificate DCCKI Certificate Profile (ordinary users)

Field Name	RFC 5759/5280 Type	Value	Reference
Issuer	Name	CN= UI DCCKICA, O=DCC-, C=UK	

Interpretation

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

subjectKeyIdentifier

Calculated using method 2 of section 4.2.1.2 of ~~of~~ RFC 5280.

Personnel Authentication Certificate DCCKI Certificate Profile (Administration Users)

Interpretation

subjectKeyIdentifier

Calculated using method 2 of section 4.2.1.2 of ~~of~~ RFC 5280.

UI DCCKICA Certificate DCCKI Certificate Profile

<u>Field Name</u>	<u>RFC 5759/5280 Type</u>	<u>Value</u>	<u>Reference</u>
subjectKeyIdentifier	KeyIdentifier	Calculated by CA	

Appendix X 'Registration Data Interface Specification'

These changes have been redlined against Appendix X version 4.0.

Amend Appendix X 'Definitions' as follows (housekeeping change):

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 Enrolled <u>Active</u> , Suspended <u>Non-Active</u> or Withdrawn <u>Installed but not Commissioned</u> .
-------------------------	---

Amend Appendix X3 as follows (housekeeping change):

3. **INTERFACE FILES**

General Obligations

- 3.8 Each Electricity Registration Data Provider shall provide any files containing Registration Data utilising the FTPS connection or via an alternative means as agreed between the DCC and the Electricity Registration Data Provider (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).
- 3.9 Each Gas Registration Data Provider shall provide any files containing Registration Data utilising the FTPS connection or via an alternative means as agreed between the DCC and the Gas Registration Data Provider (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).
- 3.10 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).

Appendix Z ‘CPL Requirements Document’

These changes have been redlined against Appendix Z version 4.0.

Amend Appendix Z 6 as follows (housekeeping change):

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 withdrawn or cancelled by NCSC, 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 expiry, cancellation or withdrawal 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 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.
- 6.5 For the purposes of Section M8.1(~~hg~~) (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.

Appendix AB 'Service Request Processing Document'

These changes have been redlined against Appendix AB version 6.0.

Amend Appendix AB16 as follows (housekeeping change):

16 **Obligations of a SMETS1 Service Provider: Countersigned Service Request Processing**

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.

Appendix AG 'SMETS1 Transition and Migration Approach Document'

These changes have been redlined against Appendix AL version 18.0.

Amend Appendix AG 5 as follows (housekeeping change):

5. **BUSINESS CONTINUITY AND DISASTER RECOVERY**

5.2. **Business Continuity and Disaster Recovery Procedures** **Disaster Recovery**

Disaster ID	DCC Disaster Impact	DCC Mitigation	DCC Recovery Action	Incident Party Impact	Incident Party Actions on failure, failover or fallback	Applicable to SMETS1 or 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 provided pursuant to the SMETS1 Data Services.	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 partial loss of all SMETS1 Services. Incident Parties may experience a loss of some SMETS1 transactions to a particular SISP. On restart the DCC may impose systems-driven Restrictions on transaction volumes/types.	Upon restoration of impacted Services, Incident Parties shall resubmit any that have failed SMETS1 Service Requests.	SMETS1
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	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 fallback 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	SMETS1 and SMETS2+

		communication services.			(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 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: - fail over to the secondary data centre; or - 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 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.	The DCC shall do one or more of the following: - recover connection at the primary data centre; - recover connection at the secondary data centre; - recover User connection.	Incident Parties will experience loss of connectivity to Services via the DCC User Gateway Connection.	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 of: In respect of SMETS2+, Service Requests and Signed Pre-Commands; and in respect of SMETS1, SMETS1 Service Requests. In the event of a Services interruption, when requested by the DCC, Incident Parties shall only submit Category 1 Incidents. Upon restoration of impacted Services, Incident Parties may recommence submission (including submitting any that have failed) of:	SMETS1 and SMETS2+

					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 fallback to the primary data centre.	- 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. - Upon restoration of impacted Services, Incident Parties may recommence submission of Service Requests and Signed Pre-Commands (including submitting any that have failed). - Incident Parties may need to log in to the Self Service Interface again. - 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+

Table 3 – Disaster Recovery Procedures

Business Continuity

Business Continuity ID	DCC BC Impact	DCC Mitigation	DCC Recovery Action	Incident Party Impact	Incident Party Actions on failure, failover or fallback
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: - Capture orders using electronic or paper forms; - Restore the system from backups; and - 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.	- In the event of a service interruption, Incident Parties shall submit orders as requested by the DCC. - No action is required from Incident Parties on restoration of the system.

Table 4 – Business Continuity Procedures

Appendix A1 ‘Self-Service Interface Code of Connection’

These changes have been redlined against Appendix A1 version 2.0.

Amend Appendix A1 ‘Definitions’ as follows (housekeeping change):

Definitions

In this document, except where the context otherwise requires:

- expressions defined in ~~s~~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 Credentials Request	has the meaning given to that expression in the DCCKI RAPP.
--	---

Appendix AJ 'SEC Variation Testing Approach Document (SVTAD)'

These changes have been redlined against Appendix AJ version 2.0.

Amend Appendix AJ 'Definitions' as follows (housekeeping change):

6. Test Phase Description

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.

Appendix AL ‘SMETS1 Transition and Migration Approach Document’

These changes have been redlined against Appendix AL version 18.0.

Amend Appendix AL 3.15(b) as follows (housekeeping change):

3. Transitional Application of Sections of the Code

Application of Section H (DCC Services)

3.15 Whilst this TMAD remains in force:

- (a) ~~[Not used] As soon as reasonably practical after this TMAD comes into effect, each User shall provide the DCC with an additional forecast under Section H3.22 (Managing Demand for DCC User Interface Services) of the number of Service Requests in respect of SMETS1 Devices that the User will send in each of the 8 months following the end of the month in which such forecast is provided;~~
- (b) Section H8.3~~(ab)~~ (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.

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

These changes have been redlined against Appendix AN version 1.0.

Amend Appendix AN3 as follows (housekeeping change):

3 November 2020 Testing Approach Documents

- 3.6 The November 2020 DCC Test 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 BEIS Q4 2020 SEC Variations, it shall be referred to the Secretary of State for determination whose decision shall be final and binding.

Appendix AO 'S1SPKM Compliance Policy'

These changes have been redlined against Appendix AO version 1.0.

Amend Appendix AO 1.1 as follows (housekeeping change):

1 INTRODUCTION

1.1 The document comprising this Appendix ~~XX~~AO:

Amend Appendix AO 5.2(c) as follows (housekeeping change):

5. Subsequent Assurance Assessments

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 ~~SMKI~~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.

Appendix AP 'FOC S1SPKI Certificate Policy'

These changes have been redlined against Appendix AP FOC version 1.0.

Amend Appendix AP5.1.1 as follows (housekeeping change):

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 Guidance on Protective Monitoring~~~~SMKI PMA Guidance 003~~; or
 - (ii) any equivalent to the ~~SMKI PMA Guidance on Protective Monitoring~~~~SMKI PMA Guidance 003~~ 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

Amend Appendix AP5.4.2 as follows (housekeeping change):

5.4 Audit logging procedures

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~~~~SMKI PMA Guidance 003~~;
 - (ii) any equivalent to that ~~SMKI PMA Guidance on Protective Monitoring~~~~SMKI PMA Guidance 003~~ 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.

Appendix AP 'Secure S1SP Certificate Policy'

These changes have been redlined against Appendix AP Secure version 1.0.

Amend Appendix AP Secure 1 as follows (housekeeping change):

1. Introduction

1.3 Secure S1SP PKI (SS1SP PKI) participants

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

1.4 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).

Amend Appendix AP Secure 3 as follows (housekeeping change):

3. Identification and authentication

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.

Amend Appendix AP Secure 4 as follows (housekeeping change):

4. Certificate life-cycle operational requirements

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.

Amend Appendix AP Secure 10 ‘Annex A’ as follows (housekeeping change):

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
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.
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
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

Amend Appendix AP Secure 11 ‘Annex B’ as follows (housekeeping change):

11. Annex B: SS1SPCA Certificate and SS1SP End entity certificate profiles

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:

- o `id-kp-serverAuth`
 - o `id-kp-clientAuth`
 - o `id-kp-codeSigning`
- SS1SP End Entity Certificates may contain the `BasicConstraints` extension, with the following values only. `cA` must be FALSE:
 - o 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.

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

These changes have been redlined against Appendix AQ version 1.0.

Amend Appendix AQ 5 as follows (housekeeping change):

5. Test Completion for PIT and SIT

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).

Appendix AS ‘ECoS Transition and Migration Approach Document’

These changes have been redlined against Appendix AS version 1.0.

Amend Appendix AS 2 as follows (housekeeping change):

2 Defined Terms and Interpretation for the purposes of ETMAD

XML User Role MPID Signing Key	means a Private Key associated with a Public Key that is contained within an Organisation Certificate that: (a) has a Remote Party Role of “xmlSign”; and (b) has within the X520 Common Name field (with the meaning ascribed to that term in the Organisation Certificate Policy) one or two <u>Market Participant Identifier</u>unique identifiers by which the Subscriber for that Certificate may be identified in the Party Details.
--------------------------------	---

Appendix AT ‘SMETS1 Cryptographic Key Management Policy for DLMS Devices’

These changes have been redlined against Appendix AT version 1.0.

Amend Appendix AT 2 as follows (housekeeping change):

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:

b(iii) SMETS1 Symmetric Key Lifetime

(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.—

Amend Appendix AT ‘Defined terms’ as follows (housekeeping change):

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.