

This document is classified as **Clear** in accordance with the Panel Information Policy. Recipients can distribute this information to the world, there is no limit on disclosure. Information may be shared without restriction subject to copyright.

MP249 ‘House Keeping Changes 2023’

Annex A

Legal text – version 1.0

About this document

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

Section G 'Security'

These changes have been redlined against Section G version 20.0.

Amend Section G2.13 as follows:

Management of Vulnerabilities

G2.13 The DCC shall ensure that an organisation which is a CHECK approved service provider or a CREST certified tester carries out assessments that are designed to identify any vulnerability of the DCC Systems to Compromise:

- (a) in respect of each DCC System, on at least an annual basis;
- (b) in respect of each new or materially changed component or functionality of the DCC Systems, prior to that component or functionality becoming operational; and
- (c) on the occurrence of any Major Security Incident in relation to the DCC Systems.

Amend Clause G2.22B as follows:

DCC Total System: Further provisions for those parts referred to in paragraphs (b) and (c) of the definition of DCC Live Systems

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 approved service provider or a CREST certified tester but is not an organisation that:
 - (i) designed or developed any relevant system; or
 - (ii) is an Affiliate or Related Undertaking of an organisation that has designed or developed any relevant system.

Amend Section G5 as follows:

G5 INFORMATION SECURITY: OBLIGATIONS ON THE DCC AND USERS

The DCC Information Security Management System

- G5.4 The DCC Information Security Management System shall incorporate procedures that comply with:
- (a) 2021 Telecommunications (Security) Act (TSA)~~HMG Security Procedures – Telecommunications Systems and Services, Issue Number 2.2 (April 2012)~~, in respect of the security of telecommunications systems and services; or
 - (b) any equivalent to those ~~HMG s~~Security ~~p~~Procedures which update or replace them from time to time.

Amend Section G8 as follows:

Suitably Qualified Service Provider

G8.4 The User Independent Security Assurance Service Provider shall be treated as suitably qualified in accordance with this Section G8.4 only if it satisfies:

- (a) ~~one or more of~~ the requirements specified in Section G8.5; and
- (b) the requirements s specified in Section G8.6.

G8.5 The requirements specified in this Section G8.5 are that the User Independent Security Assurance Service Provider:

- ~~(a) is a CTAS provider;~~
- ~~(ab)~~ is accredited by UKAS as meeting the requirements for providing audit and certification of information security management systems in accordance with ISO/IEC 27001:2013 (Information Technology – Security Techniques – Information Security Management Systems) or any equivalent to that standard which updates or replaces it from time to time; and/or
- ~~(be)~~ holds another membership, accreditation, approval or form of professional validation that is in the

opinion of the Security Sub-Committee Panel substantially equivalent in status and effect to ~~one or more of~~ the arrangements described in paragraphs (a) ~~and (b)~~.

G8.6 The requirement specified in this Section G8.6 is that the User Independent Security Assurance Service Provider:

- (a) employs consultants who are assured under an official cyber security qualification scheme recognised by NCSC or the UK Cyber Security Council or UKAS and which is approved by the Security Sub-Committee members of the Certified Cyber Professional (CCP) and the Certified Cyber Security Consultancy (CCSC) schemes at levels equivalent to 'Chartered' 'Principal', ~~the~~ 'Lead' or 'Senior Practitioner' ~~level~~ in either the 'Security and Information Risk Advisor' or 'Information Assurance Auditor' roles; and
- (b) engages those individuals as its lead auditors for the purposes of carrying out all security assurance assessments in accordance with this Section G8.

Amend Section G9 as follows:

SUITABILITY QUALIFIED SERVICE PROVIDER

G9.5 The DCC Independent Security Assessment Service Provider shall be treated as suitably qualified in accordance with this Section G9.5 only if it satisfies:

- (a) ~~one or more of~~ the requirements specified in Section G9.6; and
- (b) the requirement specified in Section G9.7.

G9.6 The requirements specified in this Section G9.6 are that the DCC Independent Security Assessment Service Provider:

- (a) is accredited by UKAS as meeting the requirements for providing audit and certification of information security management systems in accordance with ISO/IEC 27001:2017 Information Technology – Security Techniques – Information Security Management Systems) or any equivalent to that standard which updates or replaces it from time to time; and/or
- (b) holds another membership, accreditation, approval or form of professional validation that is in the opinion of the Security Sub-Committee substantially equivalent in status and effect ~~to one or more of~~ the arrangements described in paragraphs (a) ~~and (b)~~.

G9.7 The requirement specified in this Section G9.7 is that the DCC Independent Security Assessment Service Provider:

- ~~(a)~~ ~~(a)~~ employs consultants who are assured under an official cyber security qualification scheme recognised by NCSC or the UK Cyber Security Council or UKAS and which is approved by the Security Sub-Committee certified under the Certified Cyber Security Consultancy (CCSC) scheme and have experience of operating at levels equivalent to 'Chartered', 'Principal', ~~the~~ 'Lead' or 'Senior Practitioner' ~~level~~ in either 'Security and Information Risk Advisor' or 'Information Assurance Auditor' roles; and
- (b) engages those individuals as its lead auditors for the purposes of carrying out all security assessments in accordance with this Section G7.

Section I 'Data Privacy'

These changes have been redlined against Section I version 10.0.

Amend Section I1 as follows:

I1. DATA PROTECTION AND ACCESS TO DATA

Processing of Personal Data by the DCC

- I1.6 It is acknowledged that, in providing the Services to a User, the DCC may act in the capacity of 'Data Processor' on behalf of that User in respect of the Personal Data for which that User is the 'Data Controller'.
- I1.6A The Personal Data which the DCC will Process as a Data Processor on behalf of Users will relate to Energy Consumers, and will include Personal Data which is included within messages sent and received by the DCC via the DCC User Interface or the Self-Service Interface, and/or which is included within messages sent or received by the DCC to or from Communications Hubs. The nature of such Personal Data will be that which is required or permitted to be included in such messages as described in this Code. The full description of the subject matter, the nature and purpose of the processing, and the type of personal data is as described by this Code as a whole.
- I1.7 The DCC undertakes for the benefit of each User in respect of the Personal Data for which that User is the 'Data Controller' to:
- (a) only Process that Personal Data for the purposes permitted by the DCC Licence and this Code (subject to paragraph (d) below);
 - (b) only Process that Personal Data for so long as it is required to do so by the DCC Licence and this Code;
 - (c) undertake the Processing of that Personal Data in accordance with the DCC Licence and this Code, (to the extent consistent with the DCC Licence and this Code) on the documented instructions of the User, and (subject to the foregoing requirements of this Section I1.7(c)) not in a manner that the DCC knows (or should reasonably know) is likely to cause the User to breach its obligations under the Data Protection Legislation (subject to paragraph (d) below);
 - (d) if the DCC is aware that, or is of the opinion that, any requirement of paragraph (a) (b) or (c) above infringes the Data Protection Legislation, the DCC shall immediately inform the User of this giving details of the infringement or potential infringement (unless the DCC is prohibited from doing so by any of its other obligations under Laws and Directives);
 - (e) ensure that the DCC's personnel who are authorised to Process Personal Data are under enforceable obligations of confidentiality and are required only to Process that Personal Data in accordance with the DCC's obligations under the DCC Licence and this Code;
 - (f) having regard to the state of the art, the costs of implementation and the nature, scope, context and purposes of Processing as well as the risk of varying likelihood and severity for the rights and freedoms of Data Subjects, implement appropriate technical and organisational measures to protect that Personal Data in particular from accidental or unlawful loss, destruction, alteration or unauthorised disclosure of, or access to personal data transmitted, stored or otherwise Processed (such measures to at least be in accordance with Good Industry Practice and the requirements of Section G (Security));

Managed by

- (g) taking into account the nature of the Processing assist the User with its obligations to comply with Data Subjects' requests and Data Subjects' rights under the Data Protection Legislation in respect of that Personal Data through, insofar as is possible, the use of appropriate technical and organisational measures;
- (h) taking into account the nature of the Processing and the information available to the DCC, assist the User in ensuring compliance with the User's obligations in Articles 32-36 of the General Data Protection Regulation (or its national equivalent), including:
 - (i) notifying the User without undue delay if the DCC becomes aware of a breach of the Data Protection Legislation in relation to the Personal Data (including in the event of unauthorised access to such Personal Data); and
 - (ii) providing full details of the relevant breach where caused by the DCC or any Sub-Processor without undue delay or, where necessary, in phases but always without further undue delay;
- (i) provide reasonable assistance to the User in complying with any enquiry made, or investigation or assessment initiated, by the Information Commissioner or any other Competent Authority in respect of the Processing of that Personal Data pursuant to this Code;
- (j) promptly notify the User in the event that the DCC Processes any of that Personal Data otherwise than in accordance with this Code (including in the event of unauthorised access to such Personal Data);
- (k) notify the User of any complaint relating to the DCC's obligations under the Data Protection Legislation in respect of the Processing of that Personal Data pursuant to this Code;
- (l) after the end of the provision of the Services to which the Processing of that Personal Data relates, at the written election of the User, either securely destroy the Personal Data or return it to the User together with all copies (save to the extent that the DCC is required by Laws and Directives to retain a copy of the Personal Data); and
- ~~(m)~~ permit the Independent Privacy Auditor (on the instruction of SECCo on behalf of Users collectively), on giving reasonable prior notice of its intention to audit,
- ~~(m)~~(m) to audit the DCC's compliance with this Section I1.7 during normal business hours, and shall make available to the Independent Privacy Auditor all information, systems and staff reasonably necessary for the Independent Privacy Auditor to conduct such audit. The number of audits shall be limited to no more than once in every twelve (12) calendar month period unless more frequent audits are required under the Data Protection Legislation or the Panel has grounds to suspect there has or is likely to be a breach of the Data Protection Legislation. Where practicable, DCC shall be provided with an opportunity to comment upon the scope of an audit in advance and any audit shall be carried out in such a way that interruption to DCC's operations is minimised as far as is reasonably possible.

Appendix AG ‘Incident Management Policy’

These changes have been redlined against Appendix AG version 5.0.

Amend Definitions as follows:

Definitions

In this document, except where the context otherwise requires:

- Expressions defined in section A of the Code (Definitions and Interpretation) have the same meaning as is set out in that section;
- The expressions in the left hand column below shall have the meaning given to them in the right hand column below; and
- References throughout to Service Desk mean the DCC via the Service Desk.

Business Continuity Event	An Event, other than a Disaster, that causes one or more of the ‘DCC BC Impacts’ listed in Table 4 of this document.
CPNI	Centre for the Protection of National Infrastructure
Code of Connection	One of the following Subsidiary Documents: DCC Gateway Connection Code of Connection; DCC User Interface Code of Connection; Registration Data Interface Code of Connection; Self-Service Interface Code of Connection; SMKI Code of Connection; SMKI Repository Code of Connection; DCCKI Code of Connection; DCCKI Repository Code of Connection.
Error Handling Strategy	The procedures to be followed and actions to be taken where a Service Request or the commands or responses related to it fail to provide the result expected from that type or category of Service Request as further described in clause 4
HMG	Her Majesty’s Government
Interested Party	A Party or Registration Data Provider that is or has the potential to be affected by a Problem or Incident
Known Error	A fault in a component of the DCC Total System which is used for the provision of Live Services, identified by the successful diagnosis of an Incident or Problem and for which both Root Cause and a temporary work-around or a permanent solution have been identified
Live Service	Means 1) any of the Services that the DCC is obliged to provide to a User, an Authorised Subscriber, a DCC Gateway Party (once its connection is capable of operation), but excluding Testing Services as set out in H14, and

	2) the exchange of data pursuant to Section E2.
Nominated Individual	means an individual who has been nominated by an Incident Party in accordance with clause 1.4.5 of this Incident Management Policy
Normal Business Day	means the period starting 08:00 and finishing at 18:00 on a Working Day.
Normal Business Hours	means hours during a Normal Business Day.
Root Cause	is the ultimate cause of an Incident or Problem
Root Cause Analysis	a class of problem solving methods aimed at identifying the Root Cause of a Problem or Incident
Service Alert	An alert notifying Interested Parties of a current issue which may impact the provision of Services
Target Initial Response Time	The time period within which an Incident within each Category should be recorded on the Incident Management Log and assigned to a resolver

1. Introduction

1.1. Purpose

- 1.1.1 This document details the Incident Management Policy in accordance with the requirements of Section H9. It deals with the management of Incidents, including those related to Registration Data.
- 1.1.2 Additionally, Clauses 4 and 5 cover the Error Handling Strategy and Business Continuity and Disaster Recovery respectively.

1.2. Background

- 1.2.1 The subject matter of this document is closely related to that of the Incident Management aspects of the Registration Data Interface Specification. In order to ensure an integrated solution to managing Incidents, certain common aspects of Incident Management are set out in this document and cross-referred to in the Registration Data Interface Specification.
- 1.2.2 The Registration Data Incident types are set out in the Registration Data Interface Specification.
- 1.2.3 Error conditions and how they should be handled are covered in Clause 4, the Error Handling Strategy.

1.3. Scope

- 1.3.1 The Incident Management Policy details the full Incident Management lifecycle including management and declaration of Major Incidents, Problems and escalations.

1.4. General Provisions

- 1.4.1 Incidents may be raised only by the DCC or an Incident Party and in accordance with this Incident Management Policy.
- 1.4.2 Incidents raised and managed under this Incident Management Policy may relate to any Live Service. The Testing Issue Resolution Process set out in H14.37- H14.45 shall apply for the purpose of resolving Testing Issues.
- 1.4.3 In the event that an Incident Party considers it necessary to raise an issue relating to the provision of Services but which it considers outside the scope of Live Services or Testing Services, it shall contact the DCC directly and each of that Party and the DCC shall, acting reasonably, agree between them responsibility for resolution of the issue, which shall be resolved by the responsible Party as soon as reasonably practicable.
- 1.4.4 Incidents shall be raised and recorded in the Incident Management Log in accordance with Clause 2.
- 1.4.5 Each Incident Party shall provide the DCC with, and shall subsequently provide the DCC with any changes to, a list of Nominated Individuals from their organisation who are authorised to:
 - (a) contact the DCC to raise and record in the Incident Management Log an Incident and communicate with the DCC regarding the Incident; and/or
 - (b) perform the roles identified in the escalation process defined in Clause 2.9.
- 1.4.6 Each Registration Data Provider, when providing the DCC with a list of Nominated Individuals, shall provide details of both the core operating hours for the Registration Data Provider and the Registration Data Provider's out-of-hours facility.
- 1.4.7 Each Incident Party shall ensure that only its Nominated Individuals shall contact the DCC to raise an Incident.
- 1.4.8 The DCC shall ensure that only those Nominated Individuals pursuant to Clause 1.4.5(a) shall raise an Incident.
- 1.4.9 The DCC shall implement an authentication procedure for confirming that a communication is from an Incident Party's Nominated Individual, and such procedure shall be commensurate with the risk to the Services and Data that would arise were someone other than a Nominated Individual to raise an Incident or obtain information from the Service Desk. Incident Parties shall comply with this procedure.
- 1.4.10 The DCC and each Incident Party shall each ensure that information regarding Incidents and Problems is recorded and kept up to date in the Incident Management Log as follows:
 - (a) for Major Incidents, the Incident Party shall comply with Clause 2.2.2;
 - (b) except in the case of Clause 1.4.10 (a), the Incident Party shall use the Self-Service Interface where it is able to do so and the DCC shall ensure that information provided in this way is automatically added to the Incident Management Log;

- (c) where the Incident Party is unable to use the Self-Service Interface, it shall provide information to the Service Desk by email or by phone and the Service Desk shall ensure that this information is entered into the Incident Management Log;
- (d) when an Incident is submitted by email and the Incident Party does not provide the required information as detailed in Clause 2.3, the Service Desk shall return an email to the Incident Party requesting the missing information and the Incident shall not be recorded in the Incident Management Log until the required information has been received by the Service Desk;
- (e) the Service Desk shall enter information that the DCC originates into the Incident Management Log;
- (f) the resolver shall ensure all actions to resolve the Incident are recorded in the Incident Management Log; and
- (g) In regard to items a) – f) above, the DCC and each Incident Party shall each ensure that information is as complete as is possible and is entered into the Incident Management Log as soon as is reasonably practicable.

2. INCIDENT MANAGEMENT

2.1. Pre-requisites to Raising an Incident

DCC

2.1.1 Before raising an Incident the DCC shall take all reasonable steps to ensure an Incident does not already exist for the issue.

2.1.2 Not used.

Incident Parties other than Registration Data Providers

2.1.3 For the purposes of this clause 2.1.3 and clause 2.1.4, references to “Incident Party” do not include Registration Data Providers.

Before raising an Incident with the DCC the Incident Party shall take all reasonable steps to:

- (a) where appropriate, confirm that the issue does not reside within the HAN, or the Smart Meter, or other Devices which the Incident Party is responsible for operating;
- (b) confirm that the issue does not reside within the Incident Party’s own systems and processes;
- (c) follow the guidance set out in the self-help material made available by the DCC, including checking for Known Errors and the application of any workarounds specified; and
- (d) where the party is a User and to the extent that this is possible, use the SSI or submit a Service Request to resolve the Incident in accordance with Section H9.2.

2.1.4 In the event that the activities in clause 2.1.3 have been completed and an Incident is to be raised with the DCC, where it has access to the Self-Service Interface, the Incident

Party shall check on the Self-Service Interface to establish whether an Incident has already been raised or a Service Alert issued for this issue and:

- (a) in the event that the Incident Party can reasonably determine that an Incident or Service Alert for this issue exists, the Incident Party shall notify the Service Desk who shall register the Incident Party as an Interested Party within the Incident Management Log;
- (b) in the event that the Incident Party cannot identify an existing Incident or Service Alert they shall progress to clause 2.2 to raise an Incident.

2.11. Major Incidents not Assigned to the DCC

2.11.1 In the event that a Major Incident is assigned to an Incident Party other than the DCC:

- (a) the Incident Party may request that the DCC provides reasonable assistance. When this is requested the DCC shall provide all reasonable assistance to the Incident Party responsible for resolving the Incident in accordance with Section H9.12(b); and
- (b) as part of such reasonable assistance, the DCC may disseminate the information to Incident Parties if requested by the Incident Party, using the Self-Service Interface and other mechanisms as appropriate.

4. ERROR HANDLING STRATEGY

- 4.1. The first version of the contents of the Error Handling Strategy will be the 'Error Handling Strategy – DCC Guidance Document' as published by the DCC in June 2016.
- 4.2. The DCC shall make the Error Handling Strategy available to Users through the Self-Service Interface.
- 4.3. The DCC may update the Error Handling Strategy from time to time. The DCC shall ensure that Parties are consulted prior to making any changes to the Error Handling Strategy and take into account any relevant views expressed by Parties in making any changes to it.

5.2. Business Continuity and Disaster Recovery Procedures

Disaster Recovery

5.2.1 Pursuant to the requirements of Section H10.9:

- (a) the DCC shall implement the measures in the table below under 'DCC Mitigation' to reduce the likelihood of the Disaster occurring and limit the impact in the event that a Disaster has occurred;
- (b) in the event of a Disaster, the DCC shall follow the actions in the table below detailed under 'DCC Recovery Action'; and
- (c) Incident Parties may experience the impact set out in the table below under 'Incident Party Impact' and shall follow the actions as detailed under 'Incident Party Actions on failure, failover or fallback'.

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+?
D1(a)	The DCC loses the primary data centre provided pursuant to the (data services) contract referred to in paragraph 1.2(a) of Schedule 1 of the DCC Licence.	The DCC shall provide primary and secondary data centres providing data services for the DCC Live Systems, with a resilient server configuration in the primary data centre with an active-passive configuration between data centres. All configurations and data are backed up and backups are stored offsite. There are resilient network links to the data centres providing communication services.	The DCC shall do one of the following: a. fail over to the secondary data centre; or b. recover Services at the primary data centre.	Incident Parties may experience a loss of all Services on failover to the secondary data centre and on fallback to the primary data centre, with the exception of some Testing Services which operate from the secondary data centre.	- When requested by the DCC, Incident Parties shall suspend submission of Service Requests and Signed Pre-Commands until notified that Services have been restored. - Upon restoration of impacted Services, Incident Parties may recommence submission of Service Requests and Signed Pre-Commands (including submitting any that have failed). - When requested by the DCC, the Incident Party shall take each of the actions identified in column 6, of rows D5, D8, D9, D10, D11 and D16 of this table 3 and B6, B7 and B12 of table 4 below, as relevant, when DCC fails over from or fails back to the primary data centre.	SMETS2+
D1(b)	The DCC loses the primary data centre provided pursuant to the SMETS1 Data Services contract(s).	The DCC shall provide primary and secondary data centres in order to provide data services for the DCC Live Systems, with a resilient server configuration in the primary data centre with an active-passive configuration between data centres. All configurations and data are backed up and backups are stored offsite. There are resilient network links to the data centres providing communication services.	The DCC shall do one of the following: a. fail over to the secondary data centre; or b. recover Services at the primary data centre.	Incident Parties may experience a partial loss of SMETS1 Services on failover to the secondary data centre and on fallback to the primary data centre.	Upon restoration of impacted Services, Incident Parties may recommence submission of SMETS1 Service Requests (including submitting any that have failed).	SMETS1
D2	The DCC loses the secondary data centre provided pursuant to the (data services) contract referred to in paragraph 1.2(a) of Schedule 1 of the DCC Licence.	The DCC shall provide the ability to deliver Testing Services from either the secondary or primary data centres. All configurations & data are backed up & backups are stored offsite. There are resilient network links to the data centres providing communication services.	The DCC shall do one of the following: a. recover Services at the primary data centre; or b. recover Services at the secondary data centre.	Incident Parties will experience a loss of some Testing Services. Incident Parties may experience a loss of some data within Testing Services.	- When requested by the DCC, Incident Parties shall suspend the use of Testing Services until notified that Services have been restored. - Upon Services restoration, Incident Parties may resubmit failed test messages.	SMETS2+
D3(a)	The DCC loses both the primary and secondary data centres provided pursuant to the (data services) contract referred to in paragraph 1.2(a)	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;	Incident Parties may experience a loss of all Services. Incident Parties may experience a loss of some transactions.	When requested by the DCC, Incident Parties shall suspend submission of Service Requests and Signed Pre-Commands until notified that Services have been restored.	SMETS2+

Managed by

	of Schedule 1 of the DCC Licence.		c. restore Services to new infrastructure at an alternative data centre; d. set up network links to the new data centre.	Some information related to billing and Service Levels may be lost. On restart the DCC may impose systems-driven Restrictions on transaction volumes/types.	2. Upon Services restoration, Incident Parties may resubmit failed messages.	
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 S1SP. 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
D4	DCC Services are impacted by a virus or malware	The DCC constantly monitors its environments and networks to ensure the integrity of firewalls and anti-virus measures.	The DCC shall do one or more of the following: a. halt processing and clear the virus or malware; b. failover to a secondary data centre (or primary data centre) in the case of Testing Services; c. isolate the affected system and clear the virus or malware; d. cease to process transactions from Incident Parties impacted by the virus or malware until confirmation is received that they have applied necessary measures; e. apply any software patches to its Services; or f. recover from backup.	Incident Parties may experience a loss or interruption to affected Services. The DCC may impose systems-driven restrictions on transaction volumes/types on restart. Additional impacts are detailed in column 5 of rows D2, D5 to D12 and D15 of this table.	1. When requested by the DCC, Incident Parties shall suspend use of any affected Services. 2. Prior to re-commencement of Service provision, the DCC may request that each Incident Party confirms that it has cleaned its User Systems and applied necessary measures to prevent the virus or malware reoccurring. 3. When requested by the DCC, the Incident Party shall take each of the actions identified in column 6, of rows D5, D8, D9, D10, D11 and D16 of this table 3 and B6, B7 and B12 of table 4 below, as relevant, when DCC fails over from or fails back to the primary data centre.	SMETS1 and SMETS2+
D5	The DCC's experiences a failure of the part of the DCC Systems responsible for delivering Service Requests, Commands, Responses & Alerts	The DCC shall provide primary & secondary data centres providing data services for the DCC Live Systems, with resilient server configuration in the primary data centre with an active- passive configuration between data centres. All configurations & data are backed up & backups are stored offsite. There are resilient network links to the data centres providing communication services.	The DCC shall do one of the following: a. fail over to the secondary data centre; or b. recover Services at the primary data centre.	Incident Parties may experience a loss of Communication, Enrolment and Local Command Services. Incident Parties may experience a loss of all Services, with the exception of some Testing services which operate from the secondary data centre, during failover to the secondary data centre and 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 (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. 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.	- 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. - 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. - 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	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	SMETS1 and SMETS2+

		rerouting between both data centres.			by the DCC, Incident Parties shall only submit Category 1 Incidents.	
					3. Upon restoration of impacted Services, Incident Parties may recommence submission (including submitting any that have failed) of: - In respect of SMETS2+, Service Requests and Signed Pre-Commands; and - in respect of SMETS1, SMETS1 Service Requests.	
D10	The DCC experiences a failure of the systems used to support the Self-Service Interface	The DCC shall provide primary & secondary data centres providing data services for the DCC Live Systems, with resilient server configuration in the primary data centre with an active-passive configuration between data centres. All configurations & data shall be backed up & backups are stored offsite. There are resilient network links to the DCC User Gateway Connection with automatic rerouting between both data centres.	The DCC shall do one of the following: - fail over to the secondary data centre; or - recover Services at the primary data centre.	Incident Parties would experience loss of connectivity to Services via the Self-Service Interface. Incident Parties may experience a loss of all Services, with the exception of some Testing services which operate from the secondary data centre during the failover to the secondary data centre and on failback to the primary data centre.	1. When requested by the DCC, Incident Parties shall suspend until notified that Services have been restored submission of: - In respect of SMETS2+, Service Requests and Signed Pre-Commands; and - in respect of SMETS1, SMETS1 Service Requests. 2. Upon restoration of impacted Services, Incident Parties may recommence submission of Service Requests and Signed Pre-Commands (including submitting any that have failed). 3. Incident Parties may need to log in to the Self-Service Interface again. 4. When requested by the DCC, the Incident Party shall take each of the actions identified in column 6, of rows D5, D8, D9, D11 and D16 of this table 3 and B6, B7 and B12 of table 4 below, as relevant, when DCC fails over from or fails back to the primary data centre.	SMETS1 and SMETS2+
D11(a)	The DCC experiences a failure of the connection between the service providers referred to in paragraphs 1.2(a) and 1.2(b) of Schedule 1 of the DCC Licence (DCC WAN Gateway).	The DCC shall provide primary & secondary data centres providing data services for the DCC Live Systems, with resilient server configuration in the primary data centre with an active-passive configuration between data centres. All configurations & data shall be backed up & backups are stored offsite. There are resilient network links to the data centres providing communication services. Commands, Responses & Alerts shall be cached.	The DCC shall do one of the following: - fail over to the secondary data centre; or - recover connection at the primary data centre.	Incident Parties may experience a delay or failure in the processing of Service Requests, Commands, Responses and Alerts. Incident Parties may experience a loss of all Services during the failover to the secondary data centre. Incident Parties would also experience a short impact on all Services on failback to the primary data centre.	1. When requested by the DCC, Incident Parties shall suspend submission of Service Requests and Signed Pre-Commands until notified that Services have been restored. 2. Upon restoration of impacted Services, Incident Parties may recommence submission of Service Requests and Signed Pre-Commands (including submitting any that have failed). 3. When requested by the DCC, the Incident Party shall take each of the actions identified in column 6, of rows D5, D8, D9, D10 and D16 of this table 3 and B6, B7 and B12 of table 4 below, as relevant, when DCC fails over from or fails back to the primary data centre.	SMETS2+
D11(b)	The DCC experiences a failure of the	The DCC shall provide primary & secondary data centres providing	The DCC shall do one of the following:	Incident Parties may experience a delay or failure in the processing of	Upon restoration of impacted Services, Incident Parties may recommence submission of SMETS1 Service	SMETS1

	connection between the DSP and the SMETS1 Data Service Providers (SMETS1 Management Gateway).	data services for the DCC Live Systems, with resilient server configuration in the primary data centre with an active-passive configuration between data centres. All configurations & data shall be backed up & backups are stored offsite. There are resilient network links to the data centres providing communication services. Commands, Responses & Alerts shall be cached.	a. fail over to the secondary data centre; or b. recover connection at the primary data centre.	Service Requests, Commands, Responses and Alerts. Incident Parties may experience a loss of all Services during the failover to the secondary data centre.	Requests (including submitting any that have failed).	
D12	Intentionally Blank					
D13	The DCC loses its primary data centre provided pursuant to the (SMKI) contract referred to in Schedule 1 of the DCC Licence.	The DCC shall provide instances of the SMKI service infrastructure at primary & secondary SMKI data centres in an active-passive configuration with full data replication between sites and resilient network links to the Data Service Provider. The DCC shall backup all SMKI configurations & data and shall store backups offsite.	The DCC shall do one of the following: a. fail over to the secondary data centre; or b. recover Services at the primary data centre.	Incident Parties would be unable to request new Organisational or Device Certificates during failure, failover or fallback to the primary data centre.	1. When requested by the DCC, Incident Parties shall suspend transmission of Certificate Signing Requests. 2. Upon restoration of impacted Services, Incident Parties may recommence submission of Certificate Signing Requests (including submitting any that have failed).	SMETS1 and SMETS2+
D14	The DCC loses both primary & secondary data centres provided pursuant to the (SMKI) contract referred to in Schedule 1 of the DCC Licence.	The DCC shall maintain full off-site configuration & data backups.	The DCC shall: a. Restore failed services at one of the existing datacentres; or b. restore failed Services to new infrastructure at an alternative data centre and shall then redirect network links to the alternate data centre.	Incident Parties may be unable to request new Organisational or Device Certificates.	1. When requested by the DCC, Incident Parties shall suspend submission of Certificate Signing Requests until Services have been restored. 2. Upon Services restoration, Incident Parties may resubmit failed Certificate Signing Requests.	SMETS12 and SMETS2+
D15(a)	The DCC loses both primary data centres provided pursuant to the DCO (Dual Control Organisation) contract.	The DCC shall provide primary and secondary data centres in order to provide data services for the DCC Live Systems, with a resilient server configuration in the primary data centre with an active-passive configuration between data centres. All configurations and data are backed up and backups are stored offsite. There are resilient network links to the data centres providing communication services.	The DCC shall do one of the following: a. fail over to the secondary data centre; or b. recover Services at the primary data centre.	Incident Parties may experience a partial loss of SMETS1 Services on failover to the secondary data centre and on fallback to the primary data centre.	Upon restoration of impacted Services, Incident Parties may recommence submission of SMETS1 Service Requests (including submitting any that have failed).	SMETS1

D15 (b)	The DCC loses both primary & secondary data centres provided pursuant to the (Dual Control Organisation) contract.	The DCC shall maintain full off-site configuration & data backups.	The DCC shall do one or more of the following: a. recover Services at the primary data centre; b. recover Services at the secondary data centre; c. restore Services to new infrastructure at an alternative data centre; or d. set up network links to the new data centre.	Incident Parties will experience a loss of all SMETS1 Services. Incident Parties may experience a loss of some SMETS1 transactions to a particular S1SP. On restart the DCC may impose systems-driven Restrictions on transaction volumes/types.	1. When requested by the DCC, Incident Parties shall suspend submission of all SMETS 1 Service Requests until Services have been restored. 2. Upon restoration of impacted Services, Incident Parties may recommence submission of SMETS1 Service Requests (including submitting any that have failed).	SMETS1
D16	A failure of a connection or interface between one or more Registration Data Providers (RDP) and the DCC	There are resilient network links to the Registration Data Providers from both primary and secondary data centres.	The DCC shall do one or more of the following: a. recover connection at the primary data centre; b. recover connection at the secondary data centre; c. recover connection to the Registration Data Provider; or d. Send Registration update by alternative (secure) means.	There may be a delay in the issuing of DCC Status Files.	1. Upon service restoration, Incident Parties may resubmit failed Service Requests and/or SMETS1 Service Requests. 2. When requested by the DCC, RDPs shall receive updates by alternative (secure) means.	SMETS1 and SMETS2+
D17	The DCC loses a data centre provided pursuant to the (communications services) contract referred to in paragraph 1.2(b) of Schedule 1 of the DCC Licence.	The DCC shall provide primary & secondary sites for communication services data centres in an active-active configuration. All configurations & data are backed up and backups are stored offsite. In the event of failure of one communications service data centre, Services would continue to be provided from the secondary data centre.	The DCC shall: a. restore the provision of Impacted Services at the affected communications data centre; or b. restore the provision of impacted Services at a new data centre.	There would be no impact on Incident Parties from a single communications service data centre failure. Restoration of the existing data centre will not impact Incident Parties.	1. No action would be required from Incident Parties to resolve this Incident. 2. Restoration of the existing data centre will not require action from Incident Parties.	SMETS1 and SMETS2+
D18	The DCC loses both data centres provided pursuant to the (communications services) contract referred to in paragraph 1.2(b) of Schedule 1 of the DCC Licence.	The DCC shall maintain full off-site configuration & data backups.	The DCC shall: a. restore impacted Services to new infrastructure at the affected location(s); or b. restore services at an alternative data centre(s)	Incident Parties may be unable to send Commands to Devices or receive Responses and Device Alerts via the DCC and will experience loss of some Services.	1. When requested by the DCC, Incident Parties shall suspend submission until notified that Services have been restored of: • In respect of SMETS2+, Service Requests and Signed Pre-Commands; and • in respect of SMETS1, SMETS1 Service Requests. 2. Incident Parties shall also comply with all reasonable DCC requests to assist with prioritising & phasing back transmission of Service Requests and/or SMETS1 Service Requests.	SMETS1 and SMETS2+
D19	The service provided pursuant to the contract referred to in	The DCC has significant, although not complete, overlap	The DCC shall:	Incident Parties may experience the failure of impacted Services directed to meters,	Upon Services restoration, Incident Parties may resubmit failed Service	SMETS1 and SMETS2+

	paragraph 1.2(b) of Schedule 1 of the DCC Licence experiences multiple access node failure (Failure of a single access node would not be regarded as a DCC Disaster).	between access nodes. The DCC shall ensure that access nodes are of a resilient design and that it has sufficient provision of mobile equipment and components spares to restore service within acceptable timescales.	deploy field maintenance and/or mobile equipment to restore Services.	Communications Hubs and Gas Proxy Functions in the affected area(s).	Requests and/or SMETS1 Service Requests.	
D20	Communications Hub Product Recall	The DCC has more than one source for Communications Hubs. Buffer stocks are held by the DCC and Communications Hub manufacturers.	The DCC shall: a. determine the nature and extent of the problem; and b. notify all Incident Parties of the extent of product recall required and effects on existing stocks and future supply.	This could result in Incident Parties diverting field staff to uninstall affected Communications Hubs, resulting in delays in installations. It might also impact stocks and future supply.	Incident Parties shall provide reasonable assistance to the DCC in resolving issues.	SMETS2+
D21	Loss of a site housing a DCC service function	The DCC shall have arrangements in place to resume all activity at an alternate location as part of its business continuity arrangements.	The DCC shall: a. relocate the service function to the designated recovery site & shall restore service from there; or b. recover services at existing site	Incident Parties may be unable to contact the affected service function until it has been recovered at an alternate location.	There is no action required from Incident Parties.	SMETS1 and SMETS2+
D22	Intentionally Blank					

Table 3 – Disaster Recovery Procedures

Business Continuity

5.2.2 Pursuant to the requirements of Section H10.9:

- the DCC shall implement the measures in the table below under 'DCC Mitigation' to reduce the likelihood of a Business Continuity Event occurring and limit the impact in the event that a Business Continuity Event has occurred;
- in the event of the occurrence of a Business Continuity Event, the DCC shall follow the actions in the table below detailed under 'DCC Recovery Action'; and
- Incident Parties may experience the impact set out in the table below under 'Incident Party Impact' and shall follow the actions as detailed under 'Incident Party Actions on failure, failover or fallback'.

Business Continuity ID	DCC BC Impact	DCC Mitigation	DCC Recovery Action	Incident Party Impact	Incident Party Actions on failure, failover or fallback
B6	The DCC experiences a failure of the systems used to support the provision of service management.	The DCC shall provide primary & secondary data centres providing data services for the DCC Live Systems, with resilient server configuration in the primary data centre with an active-passive configuration between data centres. All configurations & data are backed up & backups are stored offsite. There are resilient network links to the	The DCC shall do one of the following: 1. fail over to the secondary data centre; or 2. recover Services at the primary data centre; and 3. the DCC Service Desk shall capture Incidents using another method until it regains access to the Service Management System.	Incident Parties may be unable to raise incidents or access incident information via the Self-Service Interface. Incident Parties may experience a loss of all Services, with the exception of some Testing services which operate from the secondary data centre	- When requested by DCC, Incident Parties may only submit Category 1 Incidents. - Upon Services restoration, Incident Parties may submit outstanding Incidents. - When requested by the DCC, the Incident Party shall take each of the actions identified in column 6, of rows D5, D8,

		data centres providing communication services.		during the failover to the secondary data centre and on failback to the primary data centre.	D9, D10, D11 and D15 of table 3 above and B6, B7 and B12 of this table 4, as relevant, when DCC fails over from or fails back to the primary data centre.
B7	The DCC experiences a failure of the systems used to support the provision of data warehousing and reporting.	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 may experience unavailability of preconfigured reports via the Self-Service Interface. Incident Parties may experience a loss of all Services, with the exception of some Testing services which operate from the secondary data centre during the failover to the secondary data centre and on failback to the primary data centre.	- When requested by the DCC, Incident Parties shall suspend submission of Service Requests and Signed Pre-Commands until notified that Services have been restored. - Upon restoration of impacted Services, Incident Parties may recommence submission of Service Requests and Signed Pre-Commands (including submitting any that have failed). - When requested by the DCC, the Incident Party shall take each of the actions identified in column 6, of rows D5, D8, D9, D10, D11 and D15 of table 3 above and B6, B7 and B12 of this table 4, as relevant, when DCC fails over from or fails back to the primary data centre.
B12	Loss of the systems used to support Communications Hub ordering.	The DCC shall provide dual instances of the order management system in resilient configuration across primary and secondary data centres. All configurations & data are backed up with backups stored offsite. The DCC shall provide multiple network links & diverse routing.	The DCC shall do one or more of the following: - 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 AP2 ‘FOC S1SPKI Certificate Policy’

These changes have been redlined against Appendix AP2 version 2.0.

Amend Appendix AP2 as follows:

Glossary

1 Annex A: Definitions and Interpretation

Definitions	Interpretations
Activation	means the process of making the FOC S1SP HES and Operator Private Keys stored available for use.
Activation Data	means any private Data (such as a password or the Data on a smartcard) which are used to access a Security Container.
Application Service End Entity Certificate	means either an End Entity PKI Role CA Certificate or an End Entity PKI Role RA Certificate issued by an Intermediate Application Service PKI CA as set out in Annex B of this Policy.
Application Service CA	means the FOC S1SP exercising the function of the Application Service Root CA to Issue Certificates to the Intermediate Application Service PKI CA and the Intermediate Application Service PKI CA and storing and managing Private Keys associated with those functions.
Application Service CA Certificate	means either an Application Service Root CA Certificate or an Intermediate Application Service CA Certificate.
Application Service PKI	means one of the three public key infrastructures that support the operation of each of the FOC S1SP Operator Root CA, the Intermediate Operator CA and the Intermediate Enterprise CA.
Application Service Registration Authority (Application Service RA)	Means the Application Service CA exercising the function of receiving and processing Certificate Signing Requests and Certificate Revocation Requests made in accordance with Annex E: FOC S1SPKI RAPP of this Policy.
Application Service Root Certification Authority (Application Service Root CA)	means the FOC S1SP exercising the functions of each or all of three Application Service Root CAs to Issue Intermediate Application Service PKI CA Certificates to each or all of the three Intermediate Application Service PKI CAs and storing and managing Private Keys associated with that function.

Application Service Root CA Certificate	means one of the self-signed Certificate issued by the Application Service Root CA that meets the requirements of the Application Service Root CA Certificate profile set out in Annex B and which is issued in accordance with this Policy.
Archive	means the archive of Data created in accordance with Part 5.5.1 of this Policy (and “Archives” and “Archived” shall be interpreted accordingly).
Audit Log	means the audit log created in accordance with Part 5.4.1 of this Policy and the FOC S1SPKI CPS.
Authentication	means the process of establishing that an individual, Certificate, System, SMETS1 Device or Organisation is what he or it claims to be (and “Authenticate” shall be interpreted accordingly).
Authorised Subscriber	means one of the entities described as such in Annex E of this Policy.
Back-Up	means, in relation to Data which is held on any FOC S1SP HES System, the storage of a copy of that Data for the purpose of ensuring that the copy may be used (if required) to restore or replace the original Data; and “Backed-Up” is to be interpreted accordingly.
Certificate	means any public key certificate Issued under this Certificate Policy by the FOC S1SPCA or the Application Service CA, the certificate being an electronic document issued by a FOC S1SPCA that is used to prove the ownership of a Public Key. Valid Certificates under this Policy are: • FOC S1SPCA Certificates; • FOC S1SP End Entity Certificates; • Application Service CA Certificates; • Application Service End Entity Certificates.
Certification Authority	means the FOC S1SPCA and/or the Application Service CA as the context requires.
Certificate Policy (known as the ‘Policy’ in this document)	is a document which aims to state what are the different entities of a Public Key Infrastructure (PKI), their roles and their duties.
Certificate Profile	means a table bearing that title in Annex B and specifying certain parameters to be contained within a Certificate.
Certificate Revocation List Distribution Point (CDP)	means a shared location on the network that is used to store the CRLs
Certificate Re-Key	means a change to the Public Key contained within a Certificate bearing a particular serial number which results in a new Certificate being issued.
Certificate Revocation Request (CRR)	means a request for the revocation of a Certificate made to the FOC S1SPCA, submitted in accordance with the FOC S1SPKI RAPP and this Policy.

Certificate Signing Request (CSR)	means a request for a Certificate submitted by an Authorised Subscriber in accordance with the FOC S1SPKI RAPP as set out in Annex E of this Policy.
Certificate Status	Provides details of the validity of Certificates and includes Revocation information.
Cryptographic Module	Means a Security Container.
Cryptographic Processing	means the generation, storage or use of any Secret Key Material
Data	means any information, data, knowledge, figures, methodologies, minutes, reports, forecasts, images or sounds (together with any database made up of any of these) embodied in any medium (whether tangible or electronic).
Eligible Subscriber	means one of the entities described as such (and in relation to the relevant Certificate types) in Annex E of this Policy:
End Entity Operator Device Certificate	A Certificate issued by the Operator CA that meets the requirements of the End Entity Operator Device Certificate profile set out in Annex B and which is issued in accordance with this Policy.
End Entity PKI Role CA Certificate	means one of the Certificates issued by an Intermediate Application Service PKI CA that meets the requirements of the End Entity PKI Role CA Certificate profile set out in Annex B and which is issued in accordance with this Policy.
End Entity PKI Role RA Certificate	means one of the Certificates issued by an Intermediate Application Service PKI CA that meets the requirements of the End Entity PKI Role RA Certificate profile set out in Annex B and which is issued in accordance with this Policy.
End Entity Push Certificate	A Certificate issued by the Enterprise CA that meets the requirements of the End Entity Push Certificate profile set out in Annex B and which is issued in accordance with this Policy.
End Entity Server Certificate	A Certificate issued by the Enterprise CA that meets the requirements of the End Entity Server Certificate profile set out in Annex B and which is issued in accordance with this Policy.
FOC S1SP	Means any one of the following DCC Service Providers responsible for the delivery and operation of the FOC S1SPKI service: • TRILLIANT NETWORKS OPERATIONS (UK) LTD] (registered in England and Wales under number 011321639 whose registered office is at Morgan House, Madeira Walk, Windsor, Berkshire SL4 1EP acting in its capacity as a DCC Service Provider. • CAP GEMINI UK PLC (registered in England and Wales under number 00943935 whose registered office is at No. 1 Forge End, Woking, Surrey, GU21

	6DB acting in its capacity as a DCC Service Provider. (DXC) ENTSEV UK LIMITED (registered in England and Wales under number 00053419 whose registered office is at Royal Pavilion, Wellesley road, Aldershot, GU11 1PZ, acting in its capacity as a DCC Service Provider. Where they are acting in the capacity of, and exercising the functions of one or more of: (a) FOC S1SPCA; (b) the FOC S1SPKI Registration Authority; (c) and any other aspects of the wider FOC S1SPKI Systems.
FOC S1SP Authority Revocation List (FOC S1SP ARL)	means a list, produced by the FOC S1SPCA, of all FOC S1SPCA Certificates that have been revoked in accordance with this Policy.
FOC S1SP CA Certificates	Means either an Operator Root CA Certificate, an Intermediate Enterprise CA Certificate or an Intermediate Operator CA Certificate as set out in Annex B of this Policy.
FOC S1SP Certification Authority (or FOC S1SPCA)	means the Secure-FOC S1SP, acting in the capacity and exercising the functions of one or more of the: (a) FOC S1SP Operator Root CA; (b) Intermediate Operator CA; (c) Intermediate Enterprise CA; (d) FOC S1SPCA Systems; and (e) FOC S1SP PKI Registration Authority.
FOC S1SP Certificate Revocation List (FOC S1SPKI CRL)	means a list, produced by the FOC S1SPKI Intermediate CA, of all FOC S1SP End Entity Certificates that have been revoked in accordance with this Certification Policy.
FOC S1SP End Entity Certificates	means either an End Entity Server Certificate, an End Entity Push Certificate, or an End Entity Operator Device Certificate issued by a FOC S1SP CA as set out in Annex B of this Policy.
FOC S1SP Head End System	means the head end system which is used by the FOC S1SP to communicate with SMETS1 CHs.
FOC S1SP Intermediate Certification Authority (FOC S1SP Intermediate CA)	means the FOC S1SP exercising the function of the FOC S1SP Intermediate Enterprise CA and the Intermediate Operator CA to Issue FOC S1SP End Entity Certificates in accordance with Annex B of this Policy.
FOC S1SP Intermediate Certification Authority Certificate (FOC S1SP Intermediate CA Certificate)	Means either an Intermediate Enterprise CA Certificate or an Intermediate Operator CA Certificate as set out in Annex B of this Policy and Issued by the FOC S1SP Root CA in accordance with this Policy.
FOC S1SP Intermediate Certification Authority Private Key (FOC S1SP	Means either: - The Intermediate Operator CA Private Key; or - The Intermediate Enterprise CA Private Key.

Intermediate CA Private Key)	
FOC S1SP Intermediate Certification Authority Service Provider (FOC S1SP Intermediate CA SP)	Means (DXC) ENTSEV UK LIMITED (registered in England and Wales under number 00053419 whose registered office is at Royal Pavilion, Wellesley road, Aldershot, GU11 1PZ, acting in its capacity as a DCC Service Provider.
FOC S1SP Operator Root Certification Authority (CA)	means the FOC S1SP exercising the function of the FOC S1SP Operator Root CA to Issue Certificates to the FOC S1SP Operator Root CA and the FOC S1SP Intermediate CA and storing and managing Private Keys associated with those functions.
FOC S1SP Operator Root Certification Authority Service Provider (FOC S1SP Operator Root CA SP)	means CAP GEMINI UK PLC (registered in England and Wales under number 00943935 whose registered office is at No. 1 Forge End, Woking, Surrey, GU21 6DB acting in its capacity as a DCC Service Provider.
FOC S1SPKI	means the S1SPKIs operated by the FOC S1SP including the FOC S1SP Head End Systems, FOC S1SPCA Systems, personnel, policy and procedures and any public key infrastructure established (or to be established) by FOC S1SP for the purpose, among other things, of providing secure communications between FOC S1SP, the DCC and SMETS1 Devices. It also includes the Application Service PKIs.
FOC S1SPKI CA	Means the FOC S1SPCA and the Application Service CA.
FOC S1SPKI CA Certificate	Means any FOC S1SPCA Certificate and any Application Service CA Certificate.
FOC S1SPKI CA Private Key	Any Private Key associated with a Public Key contained with any FOC S1SPCA Certificate or any Application Service CA Certificate.
FOC S1SPKI CA Key Pair	A Public Key that is (or is to be) contained within any FOC S1SPCA Certificate or any Application Service CA Certificate and the associated Private Key.
FOC S1SPKI CPS	means the Certification Practice Statement describing how this PKI is operated and maintained and corresponds to this Policy
FOC S1SPKI End Entity Certificate	Means any FOC S1SPKI End Entity Certificate or any Application Service End Entity Certificate.
FOC S1SPKI Personnel	means those persons who are engaged by the FOC S1SP under this Policy, in so far as such persons carry out, or are authorised to carry out, any function of such FOC S1SPKI System or FOC S1SPCA or Application service CA but not Registration Authority functions (see FOC S1SPKI RA Personnel).
FOC S1SPKI RAPP	is set out in the SEC document set and is the Registration Authority Policy and Procedures (RAPP) for this policy document

FOC S1SPKI Registration Authority (RA)	Means the FOC S1SPKI CA exercising the function of receiving and processing Certificate Signing Requests and Certificate Revocation Requests made in accordance with Annex E: FOC S1SPKI RAPP of this Policy.
FOC S1SPKI Registration Authority Manager	means either a director of the FOC S1SP or any other person who may be identified as such in accordance with Annex E: FOC S1SPKI RAPP of this Policy.
FOC S1SPKI Registration Authority Personnel (FOC S1SPKI RA Personnel)	means those persons who are engaged by the FOC S1SP, in so far as such persons carry out, or are authorised to carry out, any function of the FOC S1SPKI Registration Authority
FOC S1SPKI Repository	For the purposes of the FOC S1SPKI, the “FOC S1SPKI Repository” means a number of Systems for storing and (subject to the provisions of this Policy) making available copies of Certificates Issued pursuant to the Policy.
Hardware Security Module (HSM)	means a security module is a physical computing device that safeguards and manages digital keys, performs encryption and decryption functions for digital signatures, strong authentication and other cryptographic functions
Intermediate Application Service PKI CA Certificate	means one of the Certificates issued by the Application Service Root CA that meets the requirements of the Intermediate Application Service PKI CA Certificate profile set out in Annex B and which is issued in accordance with this Policy.
Intermediate Enterprise Certification Authority (Intermediate Enterprise CA)	means the FOC S1SP exercising the function of the Intermediate Enterprise CA to Issue End Entity Push Certificates, End Entity Server Certificates, and of storing and managing the Private Keys associated with that function.
Intermediate Enterprise Certification Authority Certificate (Intermediate Enterprise CA Certificate)	means a Certificate in the form set out in the Intermediate Enterprise CA Certificate Profile in accordance with Annex B and Issued by the FOC S1SP Root CA to the Intermediate Enterprise CA in accordance with this Policy.
Intermediate Enterprise Certification Authority Private Key (Intermediate Enterprise CA Private Key)	means a Private Key that forms a Key Pair with a Public Key held within Intermediate Enterprise CA Certificate.
Intermediate Operator CA Certificate (Intermediate Operator CA Certificate)	means a Certificate in the form set out in the Intermediate Operator CA Certificate Profile in accordance with Annex B and Issued by the FOC S1SP Root CA to the Intermediate Operator CA in accordance with this Policy.
Intermediate Operator Certification Authority (Intermediate Operator CA)	means the FOC S1SP exercising the function of the Intermediate Operator CA to Issue End Entity Operator Device Certificates and of storing and managing the Private Keys associated with that function.
Intermediate Operator Certification Authority	means a Private Key that forms a Key Pair with a Public Key held within Intermediate Operator CA Certificate.

Private Key (Intermediate Operator CA Private Key)	
Intermediate Application Service PKI Certification Authority (Intermediate Application Service PKI CA)	means the FOC S1SP exercising the functions of each or all of the three Intermediate Application Service PKI CAs to Issue End Entity PKI Role CA Certificates and End Entity PKI Role RA Certificates and storing and managing Private Keys associated with that Function.
Operator Root CA Certificate	means one of the self-signed Certificates issued by the FOC S1SP Operator Root CA that meets the requirements of the Operator Root CA Certificate profile set out in Annex B and that has been issued in accordance with Policy.
Policy	means this FOC S1SP Certificate Policy.
Private Key	means the private part of an asymmetric Key Pair used for the purposes of public key cryptography and which is associated with a Public Key that is contained within any Certificate that is Issued (or to be Issued) in accordance with this Policy.
Private Key Material	in relation to a Private Key, means that Private Key and the input parameters necessary to establish, use and maintain it.
Privileged User	means a FOC S1SPKI Personnel or FOC S1SPKI RA Personnel who is authorised to carry out activities which involve access to resources, or Data held, on the FOC S1SPCA System and which are capable of being a means by which the FOC S1SPCA System (or are capable of being) being compromised to a material extent
Public Key	means the public part of an asymmetric Key Pair used for the purposes of public key cryptography.
Public Key Infrastructure	is a set of roles, policies, hardware, software and procedures needed to create, manage, distribute, use, store and revoke digital Certificates and manage public-key encryption
Relying Party	means any System, Device, organisation or individual that relies on a Certificate that has been Issued under this Policy.
S1SP	means SMETS1 Service Provider
S1SPKI	means any public key infrastructure established (or to be established) for the purpose, among other things, of providing secure communications between the DCC and SMETS1 Devices.
S1SPKI CA Systems	means the FOC S1SPCA Systems and the Application Service CA Systems.
Secret Key Material	means any Private Key, Shared Secret, Symmetric Key or other functionally equivalent cryptographic material (and any associated input parameter) that is generated and maintained by the FOC S1SP CA
Security Container	means a set of hardware, software and/or firmware that is designed for :

	a) the secure storage of Secret Key Material; and b) the implementation of Cryptographic Processing without revealing Secret Key Material.
Security Related Functionality	means the functionality of the FOC S1SP HES Systems which is designed to detect, prevent or mitigate the adverse effect of any security compromise of that System.
Security Sub-Committee or SSC	means the Security Sub-Committee under the Smart Energy Code
Smart Energy Code	means the code of that name maintained pursuant to the smart meter communication licences granted under the UK Gas Act 1986 and the UK Electricity Act 1989
SMETS1	means the Smart Metering Equipment Technical Specifications 1
Subject	the Subject of any Certificate is the entity identified in the subject field of that Certificate
Subscriber	the FOC S1SPKI Systems or a person engaged by the S1SPKI CA (acting on behalf of the S1SPKI CA) to which a Certificate has been Issued in accordance with the requirements of this Policy.
System	means a system for generating, sending, receiving, storing (including for the purposes of Back-Up), manipulating or otherwise processing electronic communications, including all hardware, software, firmware, databases and Data associated with issuing Certificates in accordance with this Policy.
Task Manager	is a function in the Trilliant software which instructs an API to perform specific tasks such as certificate administration services.
Timestamping	means the act that takes place when a Time-Stamping Authority, in relation to a Certificate, stamps a particular datum with an accurate indicator of the time (in hours, minutes and seconds) at which the activity of stamping takes place.
Timestamping Authority	A trusted timestamp is a timestamp issued by a Trusted Third Party (TTP) acting as a Time Stamping Authority (TSA). It is used to prove the existence of certain data before a certain point without the possibility that the owner can backdate the timestamps.
Trust Store	or Repository holding the Certificates for each trusted CA
Validity Period	means, in respect of a Certificate, the period of time for which that Certificate is intended to be valid.