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.

MP212 'Housekeeping changes 2022'

Annex A

Legal text – version 1.1

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 28.0.

Amend Section A 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 Testing Service described in Section H14.49 (Interoperability and Innovation eEvents~~) held by the DCC from time to time at its discretion to provide Device Manufacturers with a platform to test connectivity, interoperability, interchangeability and functionality between HAN Devices~~.
RF Noise Testing	means ~~a~~the ~~t~~Testing ~~s~~Service described in Section H14.46 (Radio Frequency Noise Testing)~~provided by the DCC to enable Device Manufacturers to test their Devices and ensure they meet the requirements of the ICHIS, so they do not impact the WAN or HAN performance~~.
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.
Wired Instrumented Test Communications Hubs (Wired ITCH)	means ~~a~~the ~~Test Communications Hub which is capable of sending WAN Commands through a wired interface during GFI~~ Testing Service described in Section H14.54 (Wired Instrumented Test Communications Hubs).

Section C 'Governance'

These changes have been redlined against Section C version 8.0.

Amend Section C 1 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 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 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, an~~d~~ 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 F 2 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.

Amend Section F 11 as follows (housekeeping change):

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 G 2 as follows (housekeeping change):

G2. SYSTEM SECURITY: OBLIGATIONS ON THE DCC

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~~C~~D and G2.22~~D~~E 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 G2.22~~C~~D and G2.22~~D~~E 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~~A~~B(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~~A~~B(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~~A~~B(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~~A~~B(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~~D~~E(b)(i) and (ii), including any fines or re-procurement costs.

Amend Section G 5 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 G 7 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 G 8 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 H 1 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 H 7 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 H 8 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 H 9 as follows (housekeeping change):

H9. INCIDENT MANAGEMENT

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 H 10 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 H 11 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:

~~(c)~~(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 H 12 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 H 13 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 H 14 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~~ meet~~s~~ 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),~~ which~~to~~ 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 H 16 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 J 1 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 K 6 as follows (housekeeping change):

K6A. DETERMINING FIXED CH CHARGES

Determining the Fixed CH Charges

K6A.4 [Not used]

Amend Section K 7 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.~~8~~9 or F7.10 or both applies (Ownership of and Responsibility for Communications Hub Auxiliary Equipment)) returned, or notified as lost or destroyed, for a reason which is a CH Pre-Installation DCC Responsibility;

(o) ('*CH returned and redeployed*') the number of Communications Hubs which have been returned by that Party during that Charging Period for a reason which is a CH User Responsibility, and which have been (or are intended to be) reconditioned for redeployment pursuant to Section F8 (Removal and Return of Communications Hubs);

(p) ('*CH returned not redeployed*') the number of Communications Hubs which have been returned, or notified as lost or destroyed, by that Party during that Charging Period for a reason which is a CH User Responsibility, and which have not been (and are not intended to be) reconditioned for redeployment pursuant to Section F8 (Removal and Return of Communications Hubs);

(q) (*'CH wrong returns location'*) an obligation to pay arising during that Charging Period as a result of the return by that Party of Communications Hubs to the wrong returns location as referred to in Section F8.9 (Return of Communications Hubs);

(r) ('*test comms hubs*') the number of Test Communications Hubs delivered to that Party during that Charging Period, and which have not been (and are not) returned to the DCC in accordance with Section F10.8 (Ordering, Delivery, Rejection and Returns);

(s) ('*additional CH Order Management System accounts*') the number of additional CH Order Management System accounts made available to that Party during that Charging Period in accordance with Section F5.23 (CH Order Management System Accounts);

(t) ('*shared solution Alt HAN Equipment*') the number (as measured at the end of that Charging Period) of MPANs associated with premises supplied with electricity by that Party and of MPRNs associated with premises supplied with gas by that Party, in respect of each of which

premises (except where the Alt HAN Inventory records that Party as having elected to use Opted-out Alt HAN Equipment at that time) Central Shared Solution Alt HAN Equipment is installed;

(u) ('*point-to-point Alt HAN Equipment*') the number (as measured at the end of that Charging Period) of MPANs associated with premises supplied with electricity by that Party and of MPRNs associated with premises supplied with gas by that Party, in respect of each of which premises (except where the Alt HAN Inventory records that Party as having elected to use Opted-out Alt HAN Equipment at that time) Central Point-to-Point Alt HAN Equipment is installed; 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 K 11 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:

Exit Criteria	means the criteria that must be satisfied before testing can be considered complete.

Section L 'Smart Metering Key Infrastructure and DCC Key Infrastructure'

These changes have been redlined against Section L version 14.0.

Amend Section L 3 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 M 10 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 P 1 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 T 5 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 X 'Transition'

These changes have been redlined against Section X version 9.0.

Amend Section X 1 as follows:

X TRANSITION

X1. GENERAL PROVISIONS REGARDING TRANSITION

Network Parties to become Subscribers

X1.11 [NOT IN USE]~~Prior to the commencement of the provision of Enrolment Services by the DCC pursuant to Section H5 (Smart Metering Inventory and Enrolment Services), each Network Party shall ensure that it has become a Subscriber for those Organisation Certificates which pertain to it and that are required by Responsible Suppliers for the purpose of complying with their obligations under Clause 5 (Post-Commissioning Obligations) of the Inventory Enrolment and Decommissioning Procedures.~~

Amend Section X 2 as follows:

X2. EFFECTIVE PROVISIONS AT DESIGNATION

Provisions to have Effect from Designation

X2.1 The Secretary of State shall be entitled to direct the Panel to cancel or suspend any Modification Proposal, in which case the Panel shall cancel or suspend the Modification Proposal in question and it shall not then be further progressed or implemented (or, in the case of suspension, shall not then be further progressed or implemented until the Secretary of State so directs). ~~The following Sections, Schedules and SEC Subsidiary Documents shall be effective from the date of this Code's designation (subject to the other provisions of this Section X):~~

~~(a) Section A (Definitions and Interpretation);~~

~~(b) Section B (Accession);~~

~~(c) Section C (Governance);~~

~~(d) Section D (Modification Process);~~

~~(e) Section E (Registration Data);~~

~~(f) Section K (Charging Methodology);~~

~~(g) Section M (General);~~

~~(h) Section X (Transition);~~

~~(i) Schedule 1 (Framework Agreement);~~

~~(j) Schedule 2 (Specimen Accession Agreement);~~

~~(k) Schedule 4 (Establishment of SECCo);~~

~~(l) Schedule 5 (Accession Information); and~~

(m) Schedule 6 (Specimen Form Letter of Credit).

Effectiveness of Section J

X2.2 Section J (Charges) shall be effective (subject to the other provisions of this Section X) from the earlier of:

(a) the date three months after the date of this Code's designation; or

(b) the date notified by the DCC to the other Original Parties on not less than 10 Working Days prior notice (on the basis that the DCC may only specify one such date from which date all of Section J shall be effective),

provided that the DCC shall be entitled to recover Charges in respect of the period from the designation of this Code.

Variations in respect of Section D

X2.3 Notwithstanding that Section D (Modifications) is stated in Section X2.1 to be effective, it shall, until the date designated by the Secretary of State for the purposes of this Section X2.3, apply as varied by this Section X2.3. The variations to apply pursuant to this Section X2.3 are that Section D (Modifications) is to apply subject to the following:

(a) the only Modification Proposals that may be raised are:

(i) subject to paragraph (b), a Path 2 Modification or a Path 3 Modification which is not an Urgent Proposal;

(ii) a Fast-Track Modification which is not an Urgent Proposal; and

(iii) a Modification Proposal of any type that is an Urgent Proposal;

(b) where either a Path 2 Modification or Path 3 Modification which is not an Urgent Proposal is raised, Section D (Modifications) shall apply to the Modification Proposal subject to the following variations:

(i) Section D8.20 (Communicating the Change Board Vote) shall apply as if each reference in that Section to "the Authority" referred to "the Secretary of State and the Authority";

(ii) the following provisions shall apply as if each reference in them to "the Authority" referred to "the Secretary of State": Section D8.3(a) (Effect of Change Board Decision); Section D9.2 (Path 1 Modifications and Path 2 Modifications); Section D9.3 (Send-Back Process); Section D9.4 (Path 3 Modifications); and Sections D10.5 and D10.6 (Subsequent Amendment to Implementation Timetable);

(c) any Modification Proposal that is raised by a Proposer on the basis that it is urgent, but which is subsequently determined by the Authority (as provided for in Section D4) not to be an Urgent Proposal, shall be cancelled and shall not be progressed;

(d) the Secretary of State shall be entitled to direct the Panel to cancel or suspend any Modification Proposal, in which case the Panel shall cancel or suspend the Modification Proposal in question and it shall not then be further progressed or implemented (or, in the case of suspension, shall not then be further progressed or implemented until the Secretary of State so directs); and

(e) the Change Board need not be established on the designation of this Code, but the Panel shall establish the Change Board as soon as reasonably practicable after the designation of this Code, and until the Change Board is established the Panel shall perform the function of the Change Board in respect of Modification Proposals (in which case, the Panel shall vote on

whether to approve or reject a Modification Proposal in accordance with the Panel Objectives and on the basis of a simple majority).

Variations in respect of Section E

X2.4 Notwithstanding that Section E (Registration Data) is stated in Section X2.1 to be effective, it shall, until the date designated by the Secretary of State for the purposes of this Section X2.4, apply as varied by this Section X2.4. The variations to apply pursuant to this Section X2.4 are that Section E (Registration Data) is to apply as if:

(a) the information to be provided under Sections E2.1 and E2.2 is (subject to Section X2.4(b)) in respect of each Metering Point or Supply Meter Point (as applicable):

(i) the MPAN or MPRN (as applicable);

(ii) the identity of the person Registered for that Metering Point or Supply Meter Point (as applicable);

(iii) the identity of the Gas Network Party for the network to which the Supply Meter Point relates;

(iv) whether or not the Metering Point has a status that indicates that it is energised;

(v) whether or not the Supply Meter Point has a status that indicates that gas is offtaken at that point;

(vi) the profile class (as referred to in Section E2.1) relating to each such Metering Point; and

(vii) whether the Supply Meter Point serves a Domestic Premises or a Non- Domestic Premises;

(b) the information to be provided under Section E2.2 in respect of the period until the end of the 15th of September 2015 (or such later date as the Secretary of State may direct) is capable of being provided either by reference to MPRNs or by reference to 'Supply Point Registration Numbers' (as defined in the UNC);

(c) the text at Sections E2.3 and E2.4 (Obligation on the DCC to Provide Data) was deleted;

(d) the text at Section E2.5 (Frequency of Data Exchanges) was replaced with "The Data to be provided in accordance with this Section E2 shall be provided or updated on the last Working Day of each month (or as soon as reasonably practicable thereafter), so as to show the position as at the end of the 15th day of that month" , and the variation set out in this paragraph (d) shall be capable of being cancelled with effect from different dates in respect of Sections E2.1, E2.2 and E2.3 (and the obligation in Section E2.5 to provide a full set of Data on Section E2.5 coming into full force and effect shall be an obligation to provide a full set of Data under Section E2.1, E2.2 or E2.3 on the variation to Section E2.5 being cancelled in respect of that Section);

(e) the text at Section E2.6 (Frequency of Data Exchanges) was replaced with "The Data to be provided in accordance with this Section E2 shall be provided in such format, and shall be aggregated in such manner, as the DCC may reasonably require in order to enable the DCC to comply with its obligations under the DCC Licence or this Code"; and

(f) the text at Sections E2.7 to E2.11 (inclusive) and E2.13 was deleted.[1]

[1] 1 The variation set out in this X2.4(f) ceased to apply from 6 July 2016 (see letter of 5 July 2016).

~~**Variations in respect of Section K**~~

~~X2.5 Notwithstanding that Section K (Charging Methodology) is stated in Section X2.1 to be effective, it shall, until the date designated by the Secretary of State for the purposes of this Section X2.5, apply as varied by this Section X2.5. The variations to apply pursuant to this Section X2.5 are that:~~

~~(a) in respect of the Fixed Charges payable for each of the months up to and including November 2013 (or such later month as the Secretary of State may direct), the DCC shall calculate the Fixed Charges as if there were no Export Suppliers and as if all Export Suppliers were Import Suppliers (and the DCC shall not therefore require data in respect of such months pursuant to Section E2.1 that distinguishes between Import MPANs and Export MPANs); and~~

~~(b) insofar as the Registration Data provided to the DCC under Section E2.2 is by reference to 'Supply Points' (as defined in the UNC), rather than MPRNs, the DCC may calculate the number of Mandated Smart Metering Systems (as defined in Section K11.1) by reference to the number of such Supply Points.~~

~~**Variations in respect of Section M**~~

~~X2.6 Notwithstanding that Section M (General) is stated in Section X2.1 to be effective, it shall, until the date designated by the Secretary of State for the purposes of this Section X2.6, apply as varied by this Section X2.6.~~

~~**General**~~

~~X2.7~~X2.2 Where a Section is stated in this Section X2 to apply subject to more than one variation, then the Secretary of State may:

(a) designate different dates from which each such variation is to cease to apply; and/or

(b) designate a date from which one or more such variations are to cease to apply (without prejudice to the continued application of the other such variations).

~~X2.8~~X2.3 Before designating any dates for the purpose of this Section X2, the Secretary of State must consult the Authority, the Panel and the Parties in respect of the proposed date. Such consultation must allow such period of time as the Secretary of State considers appropriate in the circumstances within which to make representations or objections with respect to the proposed date. The requirement for consultation may be satisfied by consultation before, as well as after, the designation of this Code.

Amend Section X 3 as follows:

X3. PROVISIONS TO BECOME EFFECTIVE FOLLOWING DESIGNATION

Effective Dates

~~X3.1~~ Each Section, Schedule and SEC Subsidiary Document (or any part thereof) shall be effective, unless (at the time of a provision being added or modified by the Secretary of State pursuant to section 88 of the Energy Act 2008) the Secretary of State directs that such addition or modification is not to have effect, or is not to have an effect until a later date. Where the Secretary of State directs that an addition or modification is not to have effect, the Secretary of State may subsequently designate a date from which it is to have effect.~~Each Section, Schedule and SEC Subsidiary Document (or any part thereof) not referred to in Section X2.1 or X2.2 shall only be effective from the date:~~

~~(a) set out or otherwise described in this Section X3; or~~

~~(b) designated in respect of that provision by the Secretary of State for the purpose of this Section X3.~~

~~X3.2 The following Sections, Schedules and Appendices shall be effective from the following dates (subject to the other provisions of this Section X):~~

~~(a) the following provisions of Section F (Smart Metering System Requirements) shall have effect as follows:~~

~~(i) Section F1 (Technical Architecture and Business Architecture Sub-Committee) shall have effect from the date on which this Code is first modified to include that Section;~~

~~(ii) Sections F4.1 (Operational Functionality), F4.2 to F4.4 (Interoperability with DCC Systems), F4.5 (Remote Access by the DCC), F4.6 and F4.7 (Physical Access to Devices by Parties) and F4.8 (Communications with Communications Hubs by the DCC over the SM WAN) shall have effect from the date on which this Code is first modified to include this Section X3.2(a)(ii); and~~

~~(iii) Sections F4.10 to F4.13 (inclusive) (Communications Hub Procurement) shall have effect from the date on which this Code is first modified to include those Sections;~~

~~(b) Section F5 (Communications Hub Forecasting and Orders) shall have effect from the date designated by the Secretary of State for the purposes of this Section X3.2(b);~~

~~(c) Section F10 (Test Communications Hubs) shall have effect from the date on which this Code is first modified to include that Section;~~

~~(d) Section G (Security) shall have effect from the date on which this Code is first modified to include that Section;~~

~~(e) Section I (Data Privacy) shall have effect from the date on which this Code is first modified to include Section I2 (Other User Privacy Audits);~~

~~(f) Section H7 (Elective Communication Services) shall have effect from 1 October 2018;~~

~~(g) Sections H10.1 to H10.8 (inclusive) (Emergency Suspension of Services) shall have effect from the date on which this Code is first modified to include those Sections;~~

~~(h) Section H12 (Intimate Communications Hub Interface Specification) shall have effect from the date on which this Code is first modified to include this Section X3.2(h);~~

~~(i) Section H13 (Performance Reporting) shall have effect from the date on which this Code is first modified to include this Section X3.2(i);~~

~~(j) Section H14 (Testing Services) shall have effect as follows:~~

~~(i) Section H14.8 (General: Forecasting) shall have effect from the commencement of Interface Testing;~~

~~(ii) Section H14.11 (General: SMKI Test Certificates) shall have effect from the commencement of Systems Integration Testing; and~~

(iii) all the other provisions of Section H14 (Testing Services) shall have effect:

(A) in respect of the User Entry Process Tests, from the commencement of Interface Testing;

(B) in respect of the SMKI and Repository Entry Process Tests, from the date from which the SMKI and Repository Entry Process Tests can be commenced (as set out in the SRT Approach Document);

(C) in respect of Device and User System Testing, from the commencement of End-to-End Testing;

(D) in respect of Modification Proposal implementation testing (as described in Section H14.34), from the date on which Modification Proposals that are neither Urgent Proposals nor Fast Track Modifications may first be raised under Section D (Modifications); and

(E) in respect of all other Testing Services, from the end of End-to-End Testing;

(k) Sections L1 (SMKI Policy Management Authority), L2 (SMKI Assurance), L4 (The SMKI Service Interface), L6 (The SMKI Repository Interface), L8 (SMKI Performance Standards and Demand Management), L9 (The SMKI Document Set) and L10 (The SMKI Recovery Procedure) shall have effect from the date on which this Code is first modified to include those Sections;

(l) Section N (SMETS1 Meters) shall have effect from the date on which this Code is first modified to include that Section;

(m) Section T (Testing During Transition) shall have effect from the date on which this Code is first modified to include that Section;

(n) Schedule 7 (Specimen Enabling Services Agreement) shall have effect from the date on which this Code is first modified to include that Schedule;

(o) Appendices A (SMKI Device Certificate Policy), B (SMKI Organisation Certificate Policy) and C (SMKI Compliance Policy) shall all have effect from the date on which this Code is first modified to include those Appendices; and

(p) Appendix F (Minimum Communication Services for SMETS1 Meters) shall have effect from the date on which this Code is first modified to include that Appendix.

Variations in respect of Section F

X3.3 Notwithstanding that Section F5 (Communications Hub Forecasting and Orders) is stated in Section X3.2 to be effective from a date to be designated, it shall apply once effective as varied by this Section X3.3. For the purposes of this Section X3.3, the "**Initial Delivery Date**" shall be 1 November 2015 (or such later date as the Secretary of State may designate as such date for the purposes of this Section X3.3). The variations to apply pursuant to this Section X3.3 are that:

(a) each Supplier Party shall (and each other Party that intends to order Communications Hubs may), subject to any contrary timings specified by the Secretary of State on designating the date from which Section F5 is to have effect:

(i) submit its first Communications Hub Forecast during the month ending nine months in advance of the start of the month in which the Initial Delivery Date occurs;

(ii) submit further Communications Hub Forecasts on a monthly basis until the month ending five months in advance of the month in which the Initial Delivery Date occurs (from which time further Communications Hub Forecasts shall be submitted without reference to this Section X3.3); and

(iii) ensure that the Communications Hub Forecasts submitted pursuant to this Section X3.3 cover a 24-month period commencing with the month in which the Initial Delivery Date occurs;

(b) no Communications Order may specify a Delivery Date that is prior to the Initial Delivery Date;

(c) until 1 June 2015 (or such later date as the Secretary of State may direct for the purposes of this Section X3.3(c)):

(i) the DCC shall not be obliged to make the CH Ordering System available;

(ii) Parties shall submit the Communications Hub Forecasts required in accordance with Section X3.3(a) by a secure means of communication (as reasonably determined by the DCC) using the template made available by the DCC for such purposes (such template to be in a readily available and commonly used electronic format);

(iii) the DCC shall accept Communications Hub Forecasts submitted by other Parties in accordance with Section X3.3(c)(ii), and shall take all reasonable steps to verify that the forecasts so submitted were submitted by the Party by which they are purported to have been submitted; and

(iv) the DCC shall make the following information available to other Parties (using a readily available and commonly used electronic format), in respect of each post code area within Great Britain:

(A) that the SM WAN is expected to be available within that post code area on the date from which the Enrolment Services first become available;

(B) where the SM WAN is not expected to be available within that post code area on that date but is expected to be available within that postcode area before 1 January 2021, the date from which the SM WAN is expected to first become available within that post code area; or

(C) that the SM WAN is not expected to be available within that post code area before 1 January 2021; and

(d) (until the following information is available via the Self-Service Interface) the DCC shall (using a readily available and commonly used electronic format) make information available to the other Parties concerning any requirement to use a particular WAN Variant (and, where applicable, in combination with any particular Communications Hub Auxiliary Equipment) for any given location in order that the Communications Hub will be able to establish a connection to the SM WAN (such information to be made available as far in advance of the date from which the SM WAN is expected to be available in that location as is reasonably practicable (and, in any event, at least 8 months in advance)).

X3.3A Notwithstanding that Section F1 (Technical Architecture and Business Architecture Sub-Committee) is stated in Section X3.2 to be effective, it shall apply as varied by this Section X3.3A. The variation to apply pursuant to this Section X3.3A is that no review under Section F1.4(f) or F1.4(g) is required before the date from which Smart Meters are first capable of being Commissioned pursuant to Section H5 (Smart Metering Inventory and Enrolment Services).

~~Variations in respect of Sections G and I~~

~~X3.2 Notwithstanding that Sections G (Security) and I (Data Privacy) are stated in Section X3.2 to be effective, they shall apply as varied by this Section X3.4. The variations to apply pursuant to this Section X3.4 are that:~~

~~(a) the process to appoint the first User Independent Security Assurance Service Provider and the process to appoint the first Independent Privacy Auditor shall be run concurrently with the intent (subject to paragraph (ii) below) that one and the same person is appointed to carry out both such roles, but:~~

~~(i) for the avoidance of doubt, this requirement shall apply only in respect of the process to appoint the first person to carry out each such role; and~~

~~(ii) where it is not possible to appoint to both such roles one person who would be suitably independent (in accordance with Sections G8.7 and I2.4) in performing the functions under Sections G8 and I2 in respect of every Party, the Panel may designate another person to perform either such role to the extent necessary to ensure that a suitably independent person is available to perform those functions in relation to each Party; and~~

~~(b) the first annual SOC2 assessments pursuant to Section G9.3(b)(i) do not need to be completed until 12 months after the commencement of any Enrolment Services or Communications Services.~~

~~Variations in respect of Section L~~

~~X3.3 Notwithstanding that Section L8 (SMKI Performance Standards and Demand Management) is stated in Section X3.2 to be effective, it shall apply as varied by this Section X3.5. The variation to apply pursuant to this Section X3.5 is that Sections L8.1 (SMKI Services: Target Response Times) to L8.6 (Code Performance Measures) will not apply until the Stage 2 Assurance Report has been published (or such later date as the Secretary of State may designate for the purposes of this Section X3.5.~~

~~Provisions to be Effective Subject to Variations~~

~~X3.4 In designating the date from which a provision of this Code is to be effective for the purpose of this Section X3, the Secretary of State may direct that such provision is to apply subject to such variation as is necessary or expedient in order to facilitate achievement of the Transition Objective (which variation may or may not be specified to apply until a specified date).~~

~~X3.5 Where the Secretary of State directs that a provision of this Code is to apply subject to such a variation, the Secretary of State may subsequently designate a date from which the provision is to apply without variation.~~

~~X3.6 Where the Secretary of State directs that a provision of this Code is to apply subject to more than one such variation, then the Secretary of State may:~~

~~(a) designate different dates from which each such variation is to cease to apply; and/or~~

~~(b) designate a date from which one or more such variations are to cease to apply (without prejudice to the continued application of the other such variations).~~

General

~~X3.7~~X3.2 Before designating any dates and/or making any directions for the purpose of this Section X3, the Secretary of State must consult the Authority, the Panel and the Parties in respect of the proposed date and/or the draft direction (as applicable). Such consultation must allow such period of time as the Secretary of State considers appropriate in the circumstances within which to make representations or objections with respect to the proposed date and/or the draft direction (as applicable).

Amend Section X 4 as follows:

X4. GOVERNANCE SET-UP ARRANGEMENTS

~~**General**~~[NOT IN USE]

~~X4.1 The provisions of Section C (Governance) shall have effect subject to the provisions of this Section X4.~~

~~**Elected Members**~~

~~X4.2 The Elected Members to be appointed on the designation of this Code shall be the individuals nominated by the Secretary of State for the purposes of this Section X4.2 (chosen on the basis of the election process administered by the Secretary of State on behalf of prospective Parties prior to the designation of this Code).~~

~~X4.3 Of the persons appointed as Elected Members in accordance with Section X4.2:~~

~~(a) certain of them shall retire 12 months after the designation of this Code; and~~

~~(b) certain of them shall retire 24 months after the designation of this Code,~~

~~as specified in the document by which they are nominated by the Secretary of State for the purposes of Section X4.2.~~

~~**Panel Chair**~~

~~X4.4 There shall be no separate Panel Chair on the designation of this Code. The Panel Members shall select (and may deselect and reselect) from among the Elected Members a person to act as Panel Chair until a person is appointed as Panel Chair pursuant to Section X4.6.~~

~~X4.5 The Elected Member acting, from time to time, as Panel Chair in accordance with Section X4.4 shall retain his or her vote as a Panel Member, but shall have no casting vote as Panel Chair.~~

~~X4.6 The Panel shall appoint a separate Panel Chair by a date no later than five months after the designation of this Code. The Panel Chair shall be appointed in accordance with a process developed by the Panel for such purpose; provided that such process must be designed to ensure that:~~

~~(a) the candidate selected is sufficiently independent of any particular Party or class of Parties;~~

~~(b) the appointment is conditional on the Authority approving the candidate;~~

(c) the Panel Chair is appointed for a three-year term (following which he or she can apply to be re-appointed);

(d) the Panel Chair is remunerated at a reasonable rate;

(e) the Panel Chair's appointment is subject to Section C3.8 (Panel Member Confirmation) and terms equivalent to those set out in Section C4.6 (Removal of Elected Members); and

(f) the Panel Chair can be required to continue in office for a reasonable period following the end of his or her term of office in the event of any delay in appointing his or her successor.

X4.7 Until such time as a separate Panel Chair has been appointed pursuant to Section X4.6, the Panel Chair shall only be entitled to appoint an additional Panel Member under Section C3.6 (Panel Chair Appointee) with the unanimous approval of the Panel.

DCC Member and Consumer Members

X4.8 The DCC Member and the Consumer Members to be appointed on the designation of this Code shall be the individuals nominated as such by the Secretary of State for the purposes of this Section X4.8.

Code Administrator and Secretariat

X4.9 The Panel shall, on the designation of this Code, be deemed to have appointed as Code Administrator and Secretariat such person or persons as the Secretary of State nominates for the purposes of this Section X4.9 (chosen on the basis of the procurement process administered by the Secretary of State on behalf of the prospective Panel prior to the designation of this Code).

X4.10 As soon as reasonably practicable following the designation of this Code, the Panel shall direct SECCo to enter into contracts with such person or persons under which they are to perform the roles of Code Administrator and Secretariat. Such contracts shall be on terms and conditions approved by the Secretary of State for the purposes of this Section X4.10.

X4.11 Without prejudice to the ongoing duties of the Panel, the appointments of, and contracts with, the Code Administrator and Secretariat made in accordance with this Section X4 are deemed to have been properly made.

Recoverable Costs

X4.12 The requirement for Recoverable Costs to be provided for in, or otherwise consistent with, an Approved Budget (as set out in Section C8.2 (SEC Costs and Expenses)) shall not apply until such time as the first Approved Budget is established. The Panel shall establish the first Approved Budget (to cover the period from the designation of this Code) as soon as reasonably practicable following the designation of this Code.

Amend Section X 6 as follows:

X6. TRANSITIONAL VARIATIONS

[NOT IN USE]~~Status of this Section X6~~

~~X6.1 This Section X6 is without prejudice to Section D (Modification Process), as (where applicable) varied pursuant to Section X2.~~

~~Secretary of State's Power to Vary for Purposes of Transition~~

~~X6.2 In pursuance of facilitating the achievement of the Transition Objective, the Secretary of State may direct that such provisions of this Code as the Secretary of State may specify are to apply subject to such variations as the Secretary of State may specify.~~

~~X6.3 Such a direction shall only be validly made if it specifies a date or dates from which the specified provision or provisions shall apply without variation. The Secretary of State may subsequently designate an earlier date from which the relevant provision is to apply without variation.~~

~~X6.4 The purposes for which such directions may be made includes purposes relating to the design, trialling, testing, set-up, integration, commencement and proving of the DCC Systems and the User Systems and the processes and procedures relating to the SEC Arrangements.~~

~~X6.5 The variations referred to in Section X6.2 may suspend the application of specified provisions of this Code and/or specify additional provisions to apply in this Code, and may include variations which:~~

~~(a) add additional limitations on Liability provided for in this Code;~~

~~(b) provide for indemnities against Liabilities to which a Party might be exposed; and/or~~

~~(c) provide for the referral to, and final determination by, the Secretary of State (or, where designated by the Secretary of State for such purposes, the Panel or the Authority) of certain Disputes.~~

~~General~~

~~X6.6 Before designating any dates and/or making any directions for the purpose of this Section X6, the Secretary of State must consult the Authority, the Panel and the Parties in respect of the proposed date and/or the draft direction (as applicable). Such consultation must allow such period of time as the Secretary of State considers appropriate in the circumstances within which representations or objections may be made.~~

Amend Section X 7 as follows:

X7. TRANSITIONAL INCIDENT MANAGEMENT PROCEDURES

[NOT IN USE]~~Period of Application~~

~~X7.1 This Section X7 shall have effect from the date on which this Code is first modified to include this Section X7.~~

~~X7.2 This Section X7 shall have effect until such time as the relevant enduring policy has been incorporated into this Code (or, if later, the time from which such policy is stated in Section X3 (Provisions to Become Effective following Designation) to have effect).~~

~~X7.3 For the purposes of Section X7.2, the relevant enduring policy is the Incident Management Policy.~~

~~X7.4 [Not used]~~

~~Transitional Provisions for Incident Management~~

~~X7.5 Each Party other than the DCC that has rights and/or obligations under those Sections referred to in the definition of Services (and which are effective in accordance with Section X3 (Provisions to Become Effective following Designation)) shall provide the DCC with an up-to-date list from time to time of nominated individuals who are authorised to log Incidents on behalf of such Party, including for each such individual suitable contact details as reasonably requested by the DCC.~~

~~X7.6 Each Network Party shall ensure that its Registration Data Provider provides the DCC with an up-to-date list from time to time of nominated individuals who are authorised to log Incidents on behalf of such Registration Data Provider, including for each such individual suitable contact details as reasonably requested by the DCC.~~

~~X7.7 The individuals identified from time to time pursuant to Section X7.5 or X7.6 in respect of each Party or Registration Data Provider shall be the "Nominated Incident Contacts" for that Party or Registration Data Provider.~~

~~X7.8 Each Party shall (and each Network Party shall ensure that its Registration Data Provider shall) comply with any reasonable request of the DCC in relation to the validation of the information provided by that Party (or that Registration Data Provider) in relation to its Nominated Incident Contacts.~~

~~X7.9 The DCC shall treat the information from time to time provided to it pursuant to Section X7.5 or X7.6 as Confidential Information.~~

~~X7.10 For those Parties and Registration Data Providers that have provided details of their Nominated Incident Contacts, the DCC shall provide a means by which Incidents can be reported to the DCC and information regarding Incidents sought from the DCC (the "Interim Service Desk"), which shall include (as a minimum) one or more email addresses and telephone numbers.~~

~~X7.11 The DCC shall ensure that the Interim Service Desk operates between 08.00 hours and 18.00 hours on Working Days.~~

~~X7.12 Parties and Registration Data Providers may report Incidents with the DCC by their Nominated Incident Contacts contacting the Interim Service Desk and providing their contact details, the nature of the Incident, the time and date of the occurrence, and the impact of the Incident.~~

~~X7.13 The DCC shall determine the prioritisation of Incidents, but subject to such prioritisation shall take all reasonable steps to mitigate and resolve each Incident such that its impact on Parties is minimised.~~

~~X7.14 The DCC shall have the right to assign reasonable actions to other Parties and/or the Registration Data Providers as reasonably required by the DCC in order to assist the DCC in mitigating and/or resolving one or more Incidents. Each Party shall (and each Network Party shall ensure that its Registration Data Provider shall) comply with any such actions so assigned to them.~~

~~X7.15 The DCC shall notify any Parties and Registration Data Providers likely to be affected by an Incident of which the DCC has become aware of: the occurrence of such Incident; its priority status; progress regarding its resolution; and its resolution. The DCC shall provide such notifications to the Nominated Incident Contacts. The DCC shall provide such notification of an Incident's resolution within one Working Day following its resolution.~~

~~X7.16 The DCC shall establish a process by which Nominated Incident Contacts can discuss with DCC the priority assigned to an Incident where a Party or Registration Data Provider disagrees with the prioritisation assigned to an Incident by the DCC.~~

~~Transitional Provisions Relating to Business Continuity and Disaster Recovery~~

~~X7.17 In the event that the Interim Service Desk is unavailable and is unlikely to resume availability within two Working Days, then the DCC shall establish an alternative means of communication by which Incidents can be reported to the DCC and information regarding Incidents sought from the DCC. Such alternative means of communication must include a telephone number that can be used to contact the DCC's Incident manager in the case of disaster events.~~

~~X7.18 In the event that an alternative means of communication is established by the DCC pursuant to Section X7.17, the DCC shall notify the Parties and the Registration Data Providers of such alternative means of communication. Such notification shall be given to the Nominated Incident Contacts via (as a minimum) email (or, if email is unavailable, SMS). Such a notification shall include a brief explanation of the reason for the Interim Service Desk's unavailability and the expected time by which it will be available as normal.~~

~~X7.19 Once the Interim Service Desk is available as normal (following a period of unavailability), the DCC shall notify the Parties and the Registration Data Providers that this is the case (such notification to be given to the Nominated Incident Contacts via (as a minimum) email).~~

~~X7.20 In the event of the Interim Service Desk being unavailable for two Working Days or more, the DCC shall (within five Working Days following the Interim Service Desk's return to normal availability) compile a report on such event setting out the cause and future mitigation. The DCC shall make any such report available to Parties, Registration Data Providers and the Panel (and, upon request, to the Authority or the Secretary of State).~~

Amend Section X 8 as follows:

X8. DEVELOPING CH SUPPORT MATERIALS

[NOT IN USE]~~Overview~~

~~X8.1 The CH Support Materials are to be developed by the DCC pursuant to this Section X8.1, and incorporated into this Code pursuant to Section X5 (Incorporation of Certain Documents into this Code).~~

~~Purpose of the CH Support Materials~~

~~X8.2 The purpose of the CH Support Materials is to make provision for such matters as are specified in Sections F5 (Communications Hub Forecasting and Orders), F6 (Delivery and Acceptance of Communications Hubs), F7 (Installation and Maintenance of Communications Hubs), F8 (Removal and Return of Communications Hub), F9 (Categories of Communications Hub Responsibility), and F10 (Test Communications Hubs), and to provide further processes and detail required to facilitate the delivery, installation, maintenance and return of Communications Hubs and Test Communications Hubs pursuant to this Code.~~

~~Process to Develop Documents~~

~~X8.3 The DCC shall develop and consult on the CH Support Materials so that drafts of each document are submitted to the Secretary of State by 1 March 2015 (or by such later date as the Secretary of State may direct for the purposes of this Section X8.3).~~

~~X8.4 The procedure by which the DCC is to develop each of the documents comprising the CH Support Materials is as follows:~~

~~(a) the DCC shall, in consultation with the Parties and such other persons as are likely to be interested, produce a draft of each of the documents;~~

~~(b) where a disagreement arises with any person who is consulted with regard to any proposal as to the content of the documents, the DCC shall endeavour to reach an agreed proposal with that person consistent with the purposes of the CH Support Materials;~~

~~(c) the DCC shall send a draft of each document to the Secretary of State as soon as is practicable after it is produced, and shall when doing so provide to the Secretary of State:~~

~~(i) a statement of the reasons why the DCC considers that draft to be fit for purpose;~~

~~(ii) copies of the consultation responses received; and~~

~~(iii) a summary of any disagreements that arose during consultation and that have not been resolved by reaching an agreed proposal; and~~

~~(d) the DCC shall comply with any requirements in a direction given to it by the Secretary of State in relation to the draft document, including:~~

~~(i) any requirement to produce and submit to the Secretary of State a further draft of the document; and~~

~~(ii) any requirement as to the process to be followed by the DCC (and the time within which that process shall be completed) prior to submitting a further such draft.~~

Amend Section X 10 as follows:

X10. THRESHOLD ANOMALY DETECTION PROCEDURES

[NOT IN USE]~~Overview~~

~~X10.1 The Threshold Anomaly Detection Procedures are to be developed by the DCC pursuant to this Section X10.1, and incorporated into this Code pursuant to Section X5 (Incorporation of Certain Documents into this Code).~~

~~Purpose of the Threshold Anomaly Detection Procedures~~

~~X10.2 The purpose of the Threshold Anomaly Detection Procedures is to make provision for such matters as are described in Section G6.1 (Threshold Anomaly Detection Procedures), and to provide further processes and detail required to facilitate those matters.~~

~~Process to Develop Document~~

~~X10.3 The DCC shall develop and consult on the Threshold Anomaly Detection Procedures in accordance with Section X10.4, and submit the document to the Secretary of State by no later than the date which falls seven months prior to the commencement of Interface Testing (or by such later date as the Secretary of State may direct).~~

~~X10.4 The procedure by which the DCC is to develop the Threshold Anomaly Detection Procedures is as follows:~~

~~(a) the DCC shall, in consultation with the Parties and such other persons as are likely to be interested, produce a draft of the document;~~

~~(b) where a disagreement arises with any Party or other person with regard to any proposal as to the content of the document, the DCC shall endeavour to reach an agreed proposal with that person consistent with the purposes of the Threshold Anomaly Detection Procedures;~~

~~(c) the DCC shall send a draft of Threshold Anomaly Detection Procedures to the Secretary of State as soon as is practicable after completion of the process described in (a) and (b) above, and shall when doing so provide to the Secretary of State:~~

~~(i) a statement of the reasons why the DCC considers that draft to be fit for purpose;~~

~~(ii) copies of the consultation responses received; and~~

~~(iii) a summary of any disagreements that arose during consultation and that have not been resolved by reaching an agreed proposal; and~~

~~(d) the DCC shall comply with any requirements in a direction given to it by the Secretary of State in relation to the draft document, including:~~

~~(i) any requirement to produce and submit to the Secretary of State a further draft of the document; and~~

~~(ii) any requirement as to the process to be followed by the DCC (and the time within which that process shall be completed) prior to submitting a further such draft.~~

Section Z 'The Alt HAN Arrangements'

These changes have been redlined against Section Z version 9.0.

Amend Section Z 1 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 ~~is~~ Chair is unable to be available to perform his or her role, a reference to the Alternate Chair.

Amend Section Z 3 as follows (housekeeping change):

Z3. ALT HAN SECRETARIAT

Z3.1 A~~l~~ltHANCo 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 Section Z 'Annex' as follows (housekeeping change):

Annex – AltHANCo

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):

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 B 4 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 D 7 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 'Definitions' 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).

Amend Appendix I 5 as follows (housekeeping change):

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.

Amend Appendix I 8 as follows (housekeeping change):

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.

Amend Appendix I 10 as follows (housekeeping change):

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.

Amend Appendix I 'Annex A' as follows (housekeeping change):

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.

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

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'.

Amend Appendix I 'Annex C' as follows (housekeeping change):

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.

Amend Appendix I 'Annex E' as follows (housekeeping change):

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-GHz

Appendix J 'Enduring Testing Approach Document'

These changes have been redlined against Appendix J version 5.0.

Amend Appendix J 5 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 L 1 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 L 2 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 L 4 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: a. determine which of the steps (if any) as set out in section 4.2.2 of this document should be executed, in order to recover from the Compromise; b. confirm whether the timescales proposed by the DCC (following consultation with the affected Subscriber(s)) in step 4.3.1.5 for recovery, are approved or whether alternate timescales should apply; and c. if the SMKI PMA has determined that steps in this procedure should be undertaken, detail the actions that the Subscriber is to undertake, in terms of Private Key Deistruction 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 L 5 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: a. The DCC is to issue Commands using the Contingency Private Key, the DCC shall, where necessary, amend the relevaent Anomaly Detection Thresholds; and b. 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: a. the DCC Access Control Broker Certificate in each Supplier SMETS2+ Device Trust Anchor Cell with a replacement Organisation Certificate that is Issued under the new Issuing OCA, for each SMETS2+ Device as established in step 5.2.2 within section 5.2 of this document; and b. the DCC Access Control Broker Certificate in each Network 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 L 6 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): a. informing the requisite number of Key Custodians, via a secured electronic means, that a Key Generation Ceremony for the Contingency Key Pair, and for the Contingency Symmetric Key is required and the date, time and location of each such Key Generation Ceremony; b. notifying Key Custodians to attend the relevant Key Generation Ceremony; and c. activities required to prepare such systems environment required to support: a. generation of a new Contingency Key Pair; b. creating a new M#N Share of the Contingency Private Key; c. generation of a new Contingency Symmetric Key; d. encryption of the new Contingency Public Key using the new Contingency Symmetric Key; e. for the new symmetric key, conducting Contingency Symmetric Key Splitting; f. generation of a replacement Root OCA Certificate, containing the Public Key from the current Root OCA Certificate and the new encrypted Contingency Public Key; g.	DCC, Key Custodians	6.1.1.4

Amend Appendix L 7 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 O 1 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 O 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, ~~T~~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

Field Name	RFC 5759/5280 Type	Value	Reference
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~~Active, ~~Suspended~~Non-Active or ~~Withdrawn~~Installed but not Commissioned.

Amend Appendix X 3 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 5 as follows (housekeeping change):

5. Adding Device Models to CPA Certificates

5.1 An existing CPA Certificate for a Device Model may allow one or more additional Device Models to be added under that existing CPA Certificate, provided that any additional Device Model differs from the Device Model for which the CPA Certificate was originally issued only by virtue of having different versions of hardware and/or firmware that do not have a significant impact on the security functions of the Device Model (as set out in the CPA Assurance Maintenance Plan). Where this is the case:

(a) the DCC for Communications Hubs; or

(b) a Supplier Party for Device Models of all other Physical Device Types,

may notify the Panel of one or more additional Device Models to be added to the CPA Certificate.

5.2 Where the DCC or a Supplier Party notifies the Panel of an additional Device Model pursuant to Clause 5.1, the DCC or the Supplier Party shall:

(a) only do so in accordance with the terms of the relevant CPA Assurance Maintenance Plan; and

(b) retain evidence that it has acted in accordance with the terms of the relevant CPA Assurance Maintenance Plan, such evidence to be provided to the Panel or the Authority on request.

~~5.3~~ The Panel shall not be required to check whether the DCC or a Supplier Party (as applicable) is entitled to add a Device Model under the terms of the CPA Certificate and

5.3 the CPA Assurance Maintenance Plan (as described in Clause 5.1).

5.4 [NOT IN USE]

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 N~~S~~CSC 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(~~h~~g) (Events of Default), the obligations of a Party under Clause 6.3 are material obligations. Accordingly failure by a Party to gain approval for, or failure by a Party to comply in all material respects with, a CPA Certificate Remedial Plan shall be an Event of Default if not remedied within 20 Working Days after notice from the Security Sub-Committee requiring remedy.

Appendix AB 'Service Request Processing Document'

These changes have been redlined against Appendix AB version 6.0.

Amend Appendix AB 16 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 failback	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 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
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 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	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: a. fail over to the secondary data centre; or b. recover Services at the primary data centre.	Incident Parties would be unable to successfully send CoS Update Security Credentials Service Requests. Incident Parties may experience a loss of all Services during the failover to the secondary data centre. Incident Parties would also experience a loss of all Services on failback to the primary data centre.	1. When requested by the DCC, Incident Parties shall suspend until notified that Services have been restored: • in respect of SMETS2+, the submission of Service Requests and Signed Pre-Commands; and • in respect of SMETS1, the submission of SMETS1 Service Requests. 2. Upon restoration of impacted Services, Incident Parties may recommence submission (including submitting any that have failed) of: • in respect of SMETS2+, Service Requests and Signed Pre-Commands; and • in respect of SMETS1, SMETS1 Service Requests. 3. When requested by the DCC, the Incident Party shall take each of the actions identified in column 6, of rows D5, D9, D10, D11 and D16 of this table 3 and B6, B7 and B12 of table 4 below, as relevant, when DCC fails over from or fails back to the primary data centre.	SMETS1 and SMETS2+
D9	The DCC experiences a loss of connectivity to one or more Incident Parties	The DCC shall provide primary & secondary data centres providing data services for the DCC Live Systems, with resilient server 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: a. recover connection at the primary data centre; b. recover connection at the secondary data centre; c. 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 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+

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 failback
B12	Loss of the systems used to support Communications Hub ordering.	The DCC shall provide dual instances of the order management system in resilient configuration across primary and secondary data centres. All configurations & data are backed up with backups stored offsite. The DCC shall provide multiple network links & diverse routing.	The DCC shall do one or more of the following: 1. Capture orders using electronic or paper forms; 2. Restore the system from backups; and 3. On restoration of the system, the DCC shall ensure that all captured orders are entered.	Restoration of the CH Ordering System will -not impact Incident Parties.	1. In the event of a service interruption, Incident Parties shall submit orders as requested by the DCC. 2. No action is required from Incident Parties on restoration of the system.

Table 4 – Business Continuity Procedures

Appendix AI ‘Self-Service Interface Code of Connection’

These changes have been redlined against Appendix AI version 2.0.

Amend Appendix AI ‘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 'Glossary' as follows (housekeeping change):

Glossary

The table below defines only terms that are specifically not as defined in Section A (Definitions and Interpretations) of the SEC[2].

This document uses standard testing terminology, a glossary (Reference 1) of which can be found on the International Software Testing Qualification Board website www.istqb.org

Term	Meaning
Exit Criteria	means the criteria that must be satisfied before testing can be considered complete.
User Testing	means testing by one or more Users of all or part of any changes to the DCC Total System.

Amend Appendix AJ 6 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.

[2] https://www.smartenergycodecompany.co.uk/sec/sec-and-guidance-documents

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 2 as follows (housekeeping change):

2. Defined Terms and Interpretations

Term	Meaning
Completion Report	means a report that is produced at completion of a Test Phase setting out evidence demonstrating how the criteria for the completion of that Test Phase have been met.

Amend Appendix AL 3 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(~~a~~b) (Maintenance of the DCC Systems) shall not apply in respect of the DCC Migration Systems. The DCC may undertake Planned Maintenance of the DCC Migration Systems at any time during any day, provided that the DCC shall only undertake such maintenance when it is not likely to have an adverse impact on the ability to Migrate the number of SMETS1 Installations that the DCC has committed to Migrate on that day;

(c) Section H8.4 (Maintenance of the DCC Systems) shall be modified in respect of DCC Migration Systems, such that no later than 10 Working Days prior to the start of Planned Maintenance on the DCC's Migration Systems, the DCC makes available to Parties, to Registration Data Providers and to the Technical Architecture and Business Architecture Sub-Committee a schedule of that maintenance. Such schedule shall set out (as a minimum) the following:

(i) the proposed Maintenance activity (in reasonable detail);

(ii) the parts of the Services that will be disrupted (or in respect of which there is a Material Risk of disruption) during each such Maintenance activity;

(iii) the time and duration of each such Maintenance activity; and

(iv) any associated risk that may subsequently affect the return of normal Services.

(d) Section H8.5 shall be modified such that it also applies in respect of the schedule made available pursuant to Clause 3.15(c).

(e) Section H10.13 (Business Continuity and Disaster Recovery Targets) shall not apply in respect of a SMETS1 Loss of System Availability. Instead, the DCC shall:

(i) take all reasonable steps to ensure that the Services supported by the DCC Migration Systems are restored in accordance with the following Target Service Levels, and in any event shall ensure that the Services supported by the DCC Migration Systems are restored in accordance with the following Minimum Service Levels; and

	Target Service level	**Minimum Service Level**
Recovery Time Objective	4 hours	8 hours
Recovery Point Objective	15 minutes	30 minutes

(ii) within 21 Working Days of a SMETS1 Loss of System Availability which is not deemed to be a Major Incident, produce a report setting out:

(A) the nature, cause and impact of that SMETS1 Loss of System Availability;

(B) the action that was taken to resolve the SMETS1 Loss of System Availability;

(C) any failure to achieve the Target Service Level and/or the Minimum Service Level for the Recovery Time Objective and/or the Recovery Point Objective;

(D) whether there is likely to be a reduction in DCC External Costs as a result of any failure to meet the Target Service Level(s) and/or Minimum Service Level(s); and

(E) the steps the DCC is taking to prevent re-occurrence or continuation of that reason for the SMETS1 Loss of System Availability.

(f) The DCC shall make the report under Clause 3.15(e) available to the SEC Panel. The SEC Panel shall make the report available to Parties subject to any redactions it considers necessary to avoid a risk of Compromise to the DCC Total System, User Systems, RDP Systems and/or Devices.

(g) Section H5.8 of the Code shall be modified in accordance with the provisions of Clause 3.6 of TMAD. Where there is any conflict between Sections H5.8 to H5.9 of the Code and Clause 18 of this TMAD, Clause 18 of this TMAD shall take precedence.

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.

SEC Appendix AN 'SEC Variation Testing Approach Document for BEIS Changes included in the November 2020 SEC Release' no longer applies to the SEC and so will be removed and replaced with a placeholder document.

Amend Appendix AN as follows:

APPENDIX AN

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

[NOT IN USE]

1 Definitions and Interpretations

1.1 In this SEC Variation Testing Approach Document for BEIS Q4 2020 SEC Variations (this "**November 2020 SVTAD**"), except where the context otherwise requires, the expressions in the left-hand column within Table 1.1 shall have the meanings given to them in the right h13/11/2and column within Table 1.1. Where not defined in this November 2020 SVTAD, words beginning with a capital letter used in this document are defined in Section A of the SEC.

1.2 Where there are conflicts between this November 2020 SVTAD and the related November 2020 DCC Testing Approach Document, this November 2020 SVTAD shall take precedence.

1.3 Where obligations are expressed in respect of DCC Service Providers in this November 2020 SVTAD, these shall be construed as obligations on the DCC. Where text is included in this November 2020 SVTAD which does not explicitly place obligations on a Party, the Panel, or Testing Participant, these shall be construed as obligations on the DCC.

Table 1.1 NOVEMBER 2020 SVTAD Definitions

Term	Meaning
BEIS Q4 2020 SEC Variations	means the variations to the SEC that are planned as part of the BEIS Q4 2020 package of changes referred to in the direction contained in Annex A.
Completion Report	means a report that is produced setting out evidence demonstrating how the criteria for the completion of the testing has been met.
Exit Criteria	means the criteria that must be met in order for testing (or a phase of testing) to complete.
Modified DCC Total System	means the DCC Total System as will be modified to enable the delivery of Services as set out for the November 2020 SEC Release.
November 2020 SEC Release	means the changes to the DCC Total System and processes arising as a result of the BEIS Q4 2020 SEC Variations and other contemporaneous Modifications to this Code currently planned to be implemented together in November 2020.
TAG	means the Panel's Testing Advisory Group.
November 2020 DCC Testing Approach Document	means the testing approach document produced pursuant to Clause 3.3 for the November 2020 SEC Release.
Testing Issue Thresholds	means the maximum number of extant Testing Issues that may be permitted at test completion.
User Testing	means testing by one or more Users of all or part of any changes to the DCC Total System that form part of the November 2020 SEC Release that occur as a result of the BEIS Q4 2020 SEC Variations.
November 2020 Mandated User Testing Document	means any document prepared pursuant to Clause 3 that sets out the approach to mandatory User Testing.

2 General

2.1 This document is the SEC Variation Testing Approach Document for the BEIS Q4 2020 SEC Variations.

2.2 Section X11.7 of the Code requires that the DCC and each person other than the DCC that participates in (or is required to participate in) testing under a SEC Variation Testing Approach Document shall comply with the SEC Variation Testing Approach Document.

2.3 Section X11.8 of the Code specifies that Section H14 of the Code (Testing Services) and the Enduring Testing Approach Document shall apply in respect of testing under a SEC Variation Testing Approach Document as if such testing was a Testing Service under Section H14.34 (Modification Implementation Testing); and each participant in such testing shall be deemed to be a Testing Participant for such purposes.

2.4 This November 2020 SVTAD sets out:

(a) the framework for the testing that is required to be undertaken for BEIS Q4 2020 SEC Variations as part of the November 2020 SEC Release;

(b) the arrangements that apply to the development of the November 2020 DCC Testing Approach Document; and

(c) the rules to apply to the development of any November 2020 Mandated User Testing Document.

3 November 2020 Testing Approach Documents

3.1 Testing undertaken pursuant to this November 2020 SVTAD shall be performed by the DCC and any other Party that participates in it in accordance with Good Industry Practice.

3.2 It is acknowledged that the BEIS Q4 2020 SEC Variations are planned to be implemented as part of the November 2020 SEC Release. The DCC shall prepare a draft November 2020 DCC Testing Approach Document, which may include the approach to testing where it is required for Modifications that comprise part of the November 2020 SEC Release, and which shall set out the DCC's proposals for testing where it is required to support the BEIS Q4 2020 SEC Variations including:

(a) the proposed amendments to this Code that are the subject of the testing, an explanation of the associated changes to the DCC Total System, and the testing objective;

(b) the testing environments to be used;

(c) the requirements (if any) for security testing;

(d) the requirements (if any) for system capacity testing;

(e) the testing that shall be undertaken, both in terms of the scope of testing and the extent of testing (including negative tests) and the approach to regression testing;

(f) the applicable Testing Issue Thresholds and the process for excluding Testing Issues;

(g) the exit criteria for testing to complete successfully;

(h) any perceived risks associated with the approach to testing and the proposed mitigations;

(i) the approach to providing for assurance of the testing undertaken; and

(j) matters to be included in the November 2020 SEC Release Testing Completion Report (to be prepared pursuant to Clause 4.1).

3.3 The DCC shall submit the draft November 2020 DCC Testing Approach Document to the TAG for review (and such submission by the DCC and review by the TAG may take place prior to this Clause 3.3 coming into effect); and:

(a) where the TAG and the DCC can reach an agreement, the relevant draft November 2020 DCC Testing Approach Document shall be updated by the DCC as necessary and deemed to be final; or

(b) where the TAG and the DCC cannot reach an agreement on the approach to testing for the BEIS Q4 2020 SEC Variations, the matters of disagreement shall be referred by the DCC to the Secretary of State for determination. The Secretary of State's decision on such matters shall be final and binding for the purposes of this Code and the relevant draft November 2020 DCC Testing Approach Document shall be updated by the DCC as necessary and deemed to be final.

3.4 The DCC shall comply with the November 2020 DCC Testing Approach Document, and shall take all reasonable steps to complete the tests set out in the November 2020 DCC Testing Approach Document in accordance with the milestone plan published by the DCC for the relevant November 2020 SEC Release.

3.5 Revisions to the November 2020 DCC Testing Approach Document finalised pursuant to Clause 3.3 may, from time to time, be submitted by the DCC to the TAG for agreement in accordance with the provisions of Clause 3.3, and the provisions of Clause 3.4 shall apply (again) to the revised version of the document.

3.6 The 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.

3.7 Where the DCC considers that User testing is required prior to implementation of the BEIS Q4 2020 SEC Variations it shall set out its proposals for User testing in a draft November 2020 Mandated User Testing Document, including those Users that should be required to participate in the testing and the User Role in which they are required to participate; the approach to testing; the arrangements for test completion; the process for resolving testing disputes; and notification of test completion. In developing the November 2020 Mandated User Testing Document, the DCC shall consult with the TAG, Parties and other relevant stakeholders prior to the submission of the document to the Secretary of State.

3.8 Following consultation under Clause 7, the DCC shall submit the draft November 2020 Mandated User Testing Document to the Secretary of State, indicating:

(a) why the DCC considers the draft to be fit for purpose;

(b) copies of the consultation responses received; and

(c) any areas of disagreement that arose during the consultation process and that have not been resolved.

3.9 The DCC shall comply with any direction given by the Secretary of State to re-consider, re-consult, and/or re-submit the draft document.

3.10 Should a November 2020 Mandated User Testing Document be approved by the Secretary of State, the DCC and each Party other than the DCC that participates in (or is required to participate in) testing, as set out in such approved document, shall comply with that November 2020 Mandated User Testing Document.

4 Test Completion

4.1 Completion of the testing for the BEIS Q4 2020 SEC Variations set out in the November 2020 DCC Testing Approach Document shall only complete when the Panel determines that the Exit Criteria set out in that document for that testing have been met. When the DCC considers that such completion ought to occur, the DCC shall prepare a Completion Report (which may comprise part of a November 2020 SEC Release Completion Report) as provided for in the November 2020 DCC Testing Approach Document. The DCC shall:

(a) notify the Secretary of State, the Authority, the Panel, and the Parties that the DCC considers that testing has been completed;

(b) provide the Authority, the Panel, and the Secretary of State with copies of the Completion Report (or where one exists, the November 2020 SEC Release Completion Report), and a list of the sections of such report that the DCC considers should be redacted prior to publication; and

(c) review the supporting documentation and evidence with regards to the relevant Exit Criteria with the TAG.

4.2 The Panel shall confirm the completion of testing for the BEIS Q4 2020 SEC Variations set out in the November 2020 DCC Testing Approach Document, or shall highlight where it believes the Exit Criteria have not been met.

4.3 Where the Panel confirms the completion of testing for the BEIS Q4 2020 SEC Variations (subject to the Panel and the DCC reaching an agreement regarding resolution of any issues raised by the Panel) the Completion Report (or where one exists, the November 2020 SEC Release Completion Report) shall be updated by the DCC as necessary and deemed to be final.

4.4 Where the Panel declines to confirm the completion of testing for the BEIS Q4 2020 SEC Variations, the DCC shall update the Completion Report (or where one exists, the November 2020 SEC Release Completion Report) to reflect resolution of any issues where the DCC and the Panel reached an agreement, and the DCC shall then either:

(a) refer the matters where the Panel and the DCC are in disagreement with respect to the BEIS Q4 2020 SEC Variations to the Secretary of State for determination; or

(b) continue with testing (and Clause 3.10 onwards shall apply again).

4.5 Where a referral has been made by the DCC pursuant to Clause 3.13, the determination of the Secretary of State shall be final and binding for the purposes of this Code as follows:

(a) where the Secretary of State agrees that testing for the BEIS Q4 2020 SEC Variations is complete, the relevant Completion Report (or where one exists, the November 2020 SEC Release Completion Report) shall be updated by the DCC as necessary and the contents relating to the BEIS Q4 2020 SEC Variations shall be deemed to be final; or

(b) where the Secretary of State disagrees that testing for the BEIS Q4 2020 SEC Variations is complete, the DCC shall continue with testing (and Clause 3.10 onwards shall apply again).

4.6 The DCC shall publish the final Completion Report (or where one exists, the November 2020 SEC Release Completion Report), which shall be anonymised and redacted where directed by the Panel, on the DCC Website. The DCC shall notify the Panel, the Secretary of State, the Authority and the SEC Parties of the publication of the report.

5 Annex A – Direction Pursuant to Section X11.4 of the SEC

1. This direction is made for the purposes of the Smart Energy Code designated by the Secretary of State pursuant to the smart meter communication licences granted under the Electricity Act 1989 and the Gas Act 1986 (such code being the "**SEC**").
2. Words and expressions used in this direction shall be interpreted in accordance with Section A (Definitions and Interpretation) of the SEC.
3. Pursuant to Section X11.4 (SEC Variation Testing Approach Document) of the SEC, the Secretary of State hereby directs the DCC to develop a draft SEC Variation Testing Approach Document in respect of those variations to the SEC proposed to be made for the purposes of the "BEIS Q4 2020 Package", which are currently planned to be given legal effect on a planned go-live date of 29 November 2020.
4. For the purposes of this direction, the "BEIS Q4 2020 Package" means changes to gas and electricity supply licences, the Smart Meter Communication Licences and to the Smart Energy Code (including Schedules and SEC Subsidiary Documents) that are required to support the following:
   i) the changes referred to in section 7 of the BEIS consultation on "changes to Standard Conditions of Gas and Electricity Supply Licences, conditions of the DCC Licence, the SEC, the UNC and the MRA", published on 14 January 2020[3] (which essentially propose to amend the SEC to introduce a new type of Organisation Certificate with a Remote Party Role of "xmlSign");
   ii) the changes referred to in chapters 3 and 4 of the BEIS consultation on "the DCC's provision of an enrolment service for EDMI SMETS1 meters; changes to DCC, Electricity and Gas Supply Licence Conditions; and changes to the SEC, BSC and UNC", published on 6 April 2020 (which propose to amend the SEC to introduce functionality to support Standalone Auxiliary Proportional Controllers (SAPCs) and Auxiliary Proportional Control (APC) functionality for Electricity Smart Metering Equipment (ESME) and further arrangements relating to the Issuing of Organisation Certificates with a Remote Party Role of "xmlSign");
   iii) the associated changes to SEC Schedules and Appendices required to support the above changes. This includes an additional SMETS document as well as additional Versions of CHTS and GBCS, respective draft versions 5.0[4], 1.4 and 2.1, which have been consulted upon by BEIS and are available on the SECAS website[5]. It also includes modified versions of:
      - SEC Appendix B (SMKI Organisation Certificate Policy) a draft of which was included in the Government consultation of 6 April 2020[6].
      - SEC Appendix D (SMKI Registration Authority Policies and Procedures) a draft of which was included in the Government consultation of 6 April 2020.
      - SEC Appendix E (DCC User Interface Services Schedule) A draft of which the Government plans to consult upon in May 2020. It is expected that this will simply reflect the DCC User eligibility rules set out in DUIS Draft 4.0 published for consultation by the DCC.
      - SEC Appendix J (Enduring Testing Approach Document) – changes to which are being developed by the DCC.
      - SEC Appendix K (SMKI and Repository Test Scenarios Document) – it is yet to be confirmed whether any changes are needed to this document to support the introduction of the XML signing certificates. If they are, we are expecting DCC to lead on developing any necessary changes to this document in conjunction with its development of changes to CTSD and ETAD).
      - SEC Appendix M (SMKI Interface Design Specification) a draft of which was included in the Government consultation of 6 April 2020.
      - SEC Appendix R (Common Test Scenarios Document) – changes to which are being developed by the DCC.

[3] https://smartenergycodecompany.co.uk/latest-news/consultation-on-changes-to-standard-conditions-of-gas-and-electricity-supply-licenses-conditions-of-the-dcc-licence-the-sec-the-unc-and-the-mra/

[4] Please note that BEIS intends to further consult on a device-level versioning version of this document in May. This will not include any proposals for functional change.

[5] https://smartenergycodecompany.co.uk/the-developing-sec/

[6] https://smartenergycodecompany.co.uk/latest-news/beis-consultation-on-the-dccs-provision-of-an-enrolment-service-for-edmi-smets1-meters-changes-to-dcc-electricity-and-gas-supply-licence-conditions-and-changes-to-the-sec-bscs-and-unc/

- SEC Appendix AB (Service Request Processing Document) – minor changes to which the Government proposes to consult upon in May 2020. The changes will simply reflect the fact that SAPCs are treated as if they are ESMEs for the purposes of this document.
- SEC Appendix AC (Inventory, Enrolment and Decommissioning Procedures) – changes to which the Government proposes to consult on in May 2020. Again, these changes will reflect the fact that SAPCs are treated as if they are ESMEs.

There are also new versions of the following (which include Government driven changes):

- SEC Appendix AD (DCC User Interface Services Schedule) – DCC is currently consulting on draft version 4.0 of this document.
- SEC Appendix AF (Message Mapping Catalogue) – again DCC is currently consulting on draft version 4.0 of this document.

iv) the release will also include the following Government led changes:

- changes set out in DCC CR 1277 to reinstate validation of install code lengths for SMETS1 and SMETS2+ Devices included in Service Reference Variant (SRV) 8.11; and
- changes set out in CR 1233 relating to the capture in the service audit trail of out of sequence Responses for future dated commands.

5. There may be changes to the detailed scope of the BEIS Q4 2020 Package as the project to implement it progresses and the Government will discuss any such changes with DCC. It may consequently be necessary for DCC to update the SEC Variation Testing Approach Document and/or the Testing Approach Document in accordance with the processes for the modification of those documents.
6. The Secretary of State notes that a number of other government-directed changes will be made to the SEC and licences in September 2020 but that these changes do not require changes to the DCC Total System. This includes, for example changes to support the introduction of Device-specific Technical Specification versioning.
7. Section X11.5 of the SEC sets out the required content for the draft SEC Variation Testing Approach Document, and Section X11.6 of the SEC sets out the procedures that the DCC should follow in developing it to support an approval decision by the Secretary of State.
8. The SEC Variation Testing Approach Document shall provide for the detailed test approach to be set out in an associated Testing Approach Document (TAD) to be developed by the DCC. It is acknowledged that the scope of the tests described in the TAD may also include tests that are required to support SEC Modifications that are planned to be introduced into the SEC at the same time as the BEIS Q4 2020 Release changes are to be made. The SEC Variation Testing Approach Document shall provide for the TAD to be submitted to the SEC Panel's Testing Advisory Group (TAG) for approval and, insofar as it relates to the testing of the BEIS Q4 2020 Package, for any disagreements between TAG and the DCC over the content of the TAD to be submitted for a final and binding determination by the Secretary of State.
9. A draft of the SEC Variation Testing Approach Document should be submitted by the DCC to the Secretary of State in accordance with the requirements of Section X11.6 of the SEC on or before 30 June 2020.
10. This direction is also being notified to the SEC Administrator.

Appendix AO 'S1SPKM Compliance Policy'

These changes have been redlined against Appendix AO version 1.0.

Amend Appendix AO 1 as follows (housekeeping change):

1 INTRODUCTION

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

Amend Appendix AO 5 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 'Secure S1SP Certificate Policy'

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

Amend Appendix AP 'Title' as follows (housekeeping change):

Appendix AP1

S1SPKI Certificate Policy

Secure S1SP Certificate Policy for the Secure Cohort

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

1.4Usage 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:
  - id-kp-serverAuth
  - id-kp-clientAuth
  - id-kp-codeSigning
- SS1SP End Entity Certificates may contain the BasicConstraints extension, with the following values only. cA must be FALSE:
  - End Entity
  - 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 AP 'FOC S1SPKI Certificate Policy'

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

Amend Appendix AP 'Title' as follows (housekeeping change):

Appendix AP2

S1SPKI Certificate Policy

FOC S1SPKI Certificate Policy

Amend Appendix AP 5 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 and SSC Guidance (Standards, Procedures and Guidelines)' on Protective Monitoring~~SMKI PMA Guidance 003~~; or

(ii) any equivalent to the SMKI PMA and SSC Guidance (Standards, Procedures and Guidelines) 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 AP 5 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 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 Market Participant Identifier~~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 'title page' as follows (housekeeping change):

Appendix AT

SM~~T~~ET_T_S1 Cryptographic Key Management Policy for DLMS Devices

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.