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.

# MP200 ‘Faster Switching consequential changes to the SEC’

# 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'

These changes have been redlined against Section A version 20.0.

## Include the below definitions in Section A1 in alphabetical order as follows:

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

**CSS Provider** means the entity providing the Centralised Registration Service.

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

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

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

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

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

## Amend the below definitions in Section A1 as follows:

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

(ii) any part used for a purpose specified in any of paragraphs (a) to (h) or (j) of the definition of DCC Live Systems.

**DCC Live Systems**

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

**RDP Systems**

means any Systems:
(a) which are operated by or on behalf of an Electricity Distributor or Gas Transporter responsible for providing (or procuring the provision of) Registration Data in respect of a particular MPAN or MPRN; and
(b) which are used in whole or in part for~~:~~
~~(i) the collection, storage, Back-Up, processing or communication of that Registration Data prior to, or for the purposes of, its provision to the DCC over the Registration Data Interface;~~
~~(ii)~~ generating Data for communication to the OCA, ICA or DCCKICA, or receiving Data from the OCA, ICA or DCCKICA (including any Systems which store or use Secret Key Material for such purposes),
and any other Systems from which the Systems described in paragraphs (a) and (b) are not Separated.

# Section E ‘Registration Data’

These changes have been redlined against Section E version 9.0.

## Amend Section E1.1 as follows:

## E REGISTRATION DATA

### E1. RELIANCE ON REGISTRATION DATA

**DCC**

E1.1 The DCC shall, from time to time, use and rely upon the Data previously provided to it by RDPs or provided by the CSS Provider~~to it~~ pursuant to Section E2 as most recently updated pursuant to Section E2 (~~the~~ **Registration Data**) or pursuant to Section E5 (the **Additional Registration Data**); provided that the DCC shall be allowed up to three hours from receipt to upload such Data to the DCC Systems.

## Amend Section E2 as follows:

### E2. PROVISION OF DATA

**Responsibility for Providing Electricity and Gas Registration Data**

E2.1 The CSS Provider shall provide to the DCC electricity Registration Data as required under the REC.

E2.2 The CSS Provider shall provide to the DCC gas Registration Data as required under the REC.

~~E2.1 The Electricity Network Party in respect of each MPAN relating to its network shall provide (or procure that its Registration Data Provider provides) the following information to the DCC in respect of that MPAN (insofar as such information is recorded in the relevant registration systems). The information in question is the following:~~

~~(a) the identity of the Electricity Network Party for the MPAN;~~

~~(b) whether or not the MPAN has a status that indicates that it is 'traded' (as identified in the REC), and the effective date of that status;~~

~~(c) the identity of each person which has been (at any time within the 24 months preceding the date on which the Registration Data is provided), is, or is due to become Registered in respect of the MPAN, including (to the extent applicable) the date on which each such person became or ceased to be (or is to become or ceased to be) Registered in respect of the MPAN;~~

~~(d) the identity of each person which has been (at any time within the 24 months preceding the date on which the Registration Data is provided), is, or is due to become the Meter Operator in respect of the MPAN, including (to the extent applicable) the date on which each such person became or ceased to be (or is to become or ceased to be) Meter Operator in respect of the MPAN;~~

~~(e) the address, postcode and UPRN for the Metering Point to which the MPAN relates;~~

~~(f) the direction of energy flow to or from the Metering Point to which the MPAN relates (and the date from which that direction of flow has been effective);~~

~~(g) the profile class (as defined in the REC) assigned to the MPAN, and each and every other (if any) profile class assigned to the MPAN at any time within the 24 months preceding the date on which the Registration Data is provided (including the date from and to which such profile class was effective); and~~

~~(h)~~(a) ~~details of whether an objection has been received regarding a change to the person who is to be Registered in respect of the MPAN, and whether that objection has been removed or upheld, or has resulted in the change to the person who is to be Registered being withdrawn (as at the date on which the Registration Data is provided).~~

## ~~Responsibility for Providing Gas Registration Data~~

~~E2.2 The Gas Network Party in respect of each Supply Meter Point on its network shall provide (or procure that its Registration Data Provider provides) the following information to the DCC in respect of that Supply Meter Point (insofar as such information is recorded in the relevant registration systems). The information in question is the following:~~

~~(a) the identity of the Registration Data Provider for the Supply Meter Point;~~

~~(b) the identity of the Gas Network Party for the network to which the Supply Meter Point relates, and the identity of the Gas Network Party for any network to which the Supply Meter Point related at any time within the 24 months preceding the date on which the Registration Data is provided (and the date from and to which that was the case);~~

~~(c) the MPRN for the Supply Meter Point;~~

~~(d) whether or not the Supply Meter Point has a status that indicates that gas is offtaken at that point (as identified in the UNC), and, where that status has changed since the Registration Data was last provided, notification to that effect;~~

~~(e) the identity of each person which has been (at any time within the 24 months preceding the date on which the Registration Data is provided), is, or is due to become Registered in respect of the Supply Meter Point, including (to the extent applicable) the date on which each such person became or ceased to be (or is to become or ceased to be) Registered in respect of the Supply Meter Point;~~

~~(f) the identity of each person which has been (at any time within the 24 months preceding the date on which the Registration Data is provided), is, or is due to become the Meter Asset Manager in respect of the Supply Meter Point, including (to the extent applicable) the date on which each such person became or ceased to be (or is to become or ceased to be) Meter Asset Manager in respect of the Supply Meter Point;~~

~~(g) the address, postcode and UPRN for the Supply Meter Point; and~~

~~(h) whether the Supply Meter Point serves a Domestic Premises or Non-Domestic Premises.~~

## Obligation on DCC to Provide Data to RDPs

E2.3 The DCC shall provide the information set out in Section E2.4 to the Registration Data Provider nominated by each Electricity Network Party and each Gas Network Party (as such information is further described in the Registration Data Interface Documents).

E2.4 The information to be provided by the DCC:

(a) to each Electricity Network Party's Registration Data Provider is:

(i) whether there is an Enrolled Smart Metering System associated with each of the MPANs relating to the Electricity Network Party's network (and the date of its Enrolment); and

(ii) the identity of the person which the DCC believes to be Registered in respect of each of the MPANs relating to the Electricity Network Party's network; and

(b) to each Gas Network Party's Registration Data Provider is whether there is an Enrolled Smart Metering System associated with each of the Supply Meter Points on the Gas Network Party's network (and the date of its Enrolment).

## Frequency of Data Exchanges

E2.5 ~~A full set of t~~The Data to be ~~exchanged~~ provided by the DCC to the RDPs under this Section E2 shall be provided ~~on or before the date on which this Section E2.5 comes into full force and effect (or, in the case of Registration Data Providers nominated after this Section E2.5 comes into full force and effect, shall be provided in accordance with Section E4 (RDP Entry Process)). Thereafter, the Data to be exchanged under this Section E2 shall (subject to Section E2.8) be provided~~ by way of incremental updates to Data previously provided (so that only Data that has changed is updated).

E2.6 The incremental updates to the Data to be provided in accordance with this Section E2 shall be ~~updated~~ made at the frequency and/or time required in accordance with the Registration Data Interface Documents.

~~E2.6~~E2.7 The Data to be provided by the CSS Provider under this Section E2 shall be sent as per the requirements for provisions of such data as specified in the REC.

~~E2.7 Each Electricity Network Party and each Gas Network Party shall ensure that its Registration Data Provider shall:~~

~~(a) where a full set of the Registration Data Provider's Registration Data has been requested, take all reasonable steps (including working outside of normal business hours where reasonably necessary) to provide the DCC with such data as soon as reasonably practicable following such request (and in any event within the shorter of three Working Days or four days); or~~

~~(b) where a subset of the Registration Data Provider's Registration Data has been requested, provide the DCC with the requested Data in accordance with the Registration Data Interface Documents.~~

## Registration Data Interface

E2.8 The DCC shall maintain the Registration Data Interface in accordance with the Registration Data Interface Specification, and make the interface available to the Registration Data Providers to ~~send and~~ receive Data via the DCC Gateway Connections in accordance with the Registration Data Interface Code of Connection.

E2.9 The DCC shall ensure that the Registration Data Interface is available at all times (subject to Planned Maintenance undertaken in accordance with Section H8.3).

E2.10 Each Electricity Network Party and each Gas Network Party shall ensure that its Registration Data Provider shall (when acting in such capacity) comply with the applicable obligations set out in the Registration Data Interface Documents and the Incident Management Policy.

E2.11 For the avoidance of doubt, the DCC shall comply with the applicable obligations set out in the Registration Data Interface Documents and the Incident Management Policy (as it is obliged to do in respect of all applicable provisions of this Code).

## ~~Registration Data Refreshes~~

E2.12 ~~The Registration Data Interface Documents shall provide for the means, processes and timetables for requesting and providing full and partial refreshes of the Registration Data Provider's Registration Data as required by Section E2.7.~~Not used.

E2.13 Where the DCC identifies any omissions or manifest errors in the Registration Data, the DCC shall seek to resolve any such omissions or manifest errors in accordance with the Incident Management Policy. In such circumstances, the DCC may continue (notwithstanding Section E1.1) to rely upon and use any or all of the Registration Data that existed prior to its receipt of the incremental update that included any such omission or manifest error, unless the Incident Management Policy provides for an alternative course of action.

## RDP Security Obligations~~ and RDP IDs~~

E2.14 Each Electricity Network Party and each Gas Network Party shall ensure that its Registration Data Provider (being the Network Party itself where that is deemed to be the case in accordance with the definition of Registration Data Provider) shall (when acting in its capacity as the Network Party's Registration Data Provider) comply with the obligations expressed to be placed on Users and identified in Section E2.15 as if, in the case of each such obligation:

(a) references to User were references to such Registration Data Provider; and

(b) references to User Systems were references to the RDP Systems of that Registration Data Provider.

E2.15 The obligations identified in this Section E2.15 are those obligations set out at:

(a) Sections G3.2 to G3.3 (Unauthorised Activities: Duties to Detect and Respond);

(b) Sections G3.8 to G3.9 (Management of Vulnerabilities);

(c) Sections G5.14 to G5.18 (Information Security: Obligations on Users), save that for this purpose the reference:

(i) in Section G5.18(b)(i) to "Sections G3 and G4" shall be read as if it were to "Sections G3.2 to G3.3 and G3.8 to G3.9"; and

(ii) in Section G5.18(b)(iii) to "Sections G5.19 to G5.24" shall be read as if it were to "Section G5.19(d)".

E2.16 Each Electricity Network Party and each Gas Network Party shall ensure that its Registration Data Provider (being the Network Party itself where that is deemed to be the case in accordance with the definition of Registration Data Provider) shall (when acting in its capacity as the Network Party's Registration Data Provider) propose to the DCC one or more EUI-64 Compliant identification numbers, issued to the RDP by the Panel, to be used by that RDP when acting in its capacity as such (save that it may use the same identification number when acting as an RDP for more than one Network Party).~~:~~

~~(a) Digitally Sign any communication containing Registration Data which is sent to the DCC using a Private Key associated with an Organisation Certificate for which that RDP is the Subscriber, in accordance with the requirements of the Registration Data Interface Specification;~~

~~for that purpose, propose to the DCC one or more EUI-64 Compliant identification numbers, issued to it by the Panel, to be used by that RDP when acting in its capacity as such (save that it may use the same identification number when acting as an RDP for more than one Network Party).~~

E2.17 The DCC shall accept each identification number proposed by each Registration Data Provider for the purposes set out in Section E2.16 (and record such numbers as identifying, and use such numbers to identify, such RDP when acting as such); provided that the DCC shall only accept the proposed number if it has been issued by the Panel.

## Security Obligations on CSS Provider

E2.18 The CSS Provider shall comply with the obligations expressed to be placed on Users and identified in Section E2.15 as if, in the case of each such obligation:

(a) references to User were references to the CSS Provider; and

(b) references to User Systems were references to the CSS Provider Systems.

E2.19 The CSS Provider shall ensure that any Registration Data that it sends is Digitally Signed using a Private Key that is associated with a Public Key contained within an Organisation Certificate.

E2.20 The DCC shall only use Registration Data received from the CSS Provider if:

(a) it has successfully carried out a Check Cryptographic Protection in respect of that Registration Data and successfully carried out a Confirm Validity of the Organisation Certificate used to Check Cryptographic Protection; and

~~(a)~~(b) the DCC has not previously successfully carried out the checks set out in paragraph E2.20(a) on that Registration Data.

### Disputes

E2.21 Any Dispute regarding compliance with this Section E2 may be referred to the Panel for its determination, which shall be final and binding for the purposes of this Code; save that Disputes regarding compliance with Section E2.14 shall be subject to the means of Dispute resolution applying to the provisions of Section G (Security) referred to in Section E2.15 (as set out in Section G).

### Provision of Further Data

E2.22 The Parties agree that the DCC may send the notification in Section E2.23 and the associated information set out in Section E2.24 to the CSS Provider.

E2.23 The notification referred to in Section E2.22 is a notification that a Smart Meter has been added to the Device Log of a Communications Hub.

E2.24 The information referred to in Section E2.22 is any information held in the Smart Metering Inventory that pertains to either the Communications Hub referred to in Section E2.23 or to any Smart Meter that is listed in the Device Log of that Communications Hub.

# Section G 'Security'

These changes have been redlined against Section G version 13.0.

## Add Sections G1.14 and G1.15 as follows:

**CSS Provider Systems**

G1.14 The security obligations applying to the CSS Provider Systems are set out in Section E2.18 (Security Obligations of the CSS Provider); and

G1.15 In Sections G2 to G9:

(a) other than for the purposes of Section G2.20(a), each and every reference to the DCC Total System shall exclude the CSS Provider Systems; and

~~(a)~~(b) each and every reference to the DCC Systems shall exclude the CSS Provider Systems.

# Section H 'DCC Services'

These changes have been redlined against Section H version 13.0.

## Amend Section H8.8 as follows:

### DCC Internal System Changes

H8.8 Where the DCC is proposing to make a change to DCC Internal Systems, the DCC shall:

(a) undertake an assessment of the likely impact on:

(i) Parties in respect of any potential disruption to Services; and/or

(ii) RDPs in relation to the ~~the sending or~~ receipt of data pursuant to Section E (Registration Data),

that may arise as a consequence of the Maintenance required to implement the contemplated change;

(b) where such assessment identifies that there is a Material Risk of disruption to Parties and/or RDPs, consult with Parties and/or RDPs (as applicable) and with the Technical Architecture and Business Architecture Sub-Committee regarding such risk;

(c) provide the Parties and RDPs the opportunity to be involved in any testing of the change to the DCC Internal Systems prior to its implementation; and

(d) undertake an assessment of the likely impact of the contemplated change upon the security of the DCC Total System, Smart Metering Systems, and the Systems of Parties and/or RDPs.

## Amend Section H9.6 as follows:

### Addition of Incidents to the Incident Management Log

H9.6 Where an Incident Party becomes aware of an Incident that is not yet logged on the Incident Management Log (or, if logged, is incorrectly logged as closed):

(a) (where the Incident Party is a User) to the extent such Incident is reasonably capable of being resolved via the Self-Service Interface or via a Service Request which that User has the right to send, then the User shall exercise such rights with a view to resolving the Incident;

~~(b) (where the Incident Party is an RDP) to the extent such Incident is reasonably capable of being resolved by re-submitting a subset of Registration Data in accordance with the Registration Data Interface Documents, then the RDP shall re-submit such Data; or~~

~~(c)~~(b) where ~~neither~~ paragraph (a) ~~nor (b)~~ above does not apply (or to the extent the Incident is not resolved despite compliance with paragraph (a) ~~or (b)~~ above), then the Incident Party shall add the Incident to the Incident Management Log (or, if incorrectly logged as closed, reopen the Incident) via the Self-Service Interface (or, in the case of non-Users, the Service Desk).

# Section K ‘Charging Methodology’

These changes have been redlined against Section K version 11.0.

## Amend Section K11 as follows:

**Mandated Smart Metering System** means, from time to time, each MPAN or MPRN associated with a Domestic Premises (regardless of whether or not a Smart Metering System has been installed or Enrolled), but excluding:

a. those MPANs and MPRNs associated with premises in respect of which the DCC is exempted from the requirement to Enrol Smart Metering Systems in accordance with the Statement of Service Exemptions; and

b. those MPANs and MPRNs that do not have an RMP Lifecycle Status of ‘operational ~~the status of “traded”~~ (as recorded pursuant to~~identified in~~ the REC) ~~and those MPRNs that do not have a status that indicates that gas is off-taken at the supply point (as identified in the UNC)~~.

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

These changes have been redlined against Section L version 13.0.

## Amend Section L3.18 as follows:

Organisation Certificates and OCA Certificates

L3.18 Where the DCC, a Network Party or another Party which is (or is to become) a User, or any RDP, is an Authorised Subscriber in accordance with the Organisation Certificate Policy, that person will be an Eligible Subscriber in respect of an Organisation Certificate or OCA Certificate only where:

(a) if the Subject of that Certificate is:

(i) either the DCC (acting pursuant to its powers or duties under the Code) or a DCC Service Provider, that person is the DCC; or

(ii) not the DCC, that person is the Subject of the Certificate; and

(b) if the value of the X520OrganizationalUnitName field in that Certificate is a Remote Party Role corresponding to that listed in the table immediately below, either:

(i) that person is the DCC, it is the Party identified with that Remote Party Role in the second column of that table, the Certificate Signing Request originates from the individual System referred in the paragraph of the definition of DCC Live Systems identified in the fourth column of that table, and the Certificate is to be issued to the same individual System from which the Certificate Signing Request originates; or

(ii) that person is identified with that Remote Party Role in the second column of that table, and the value of the subjectUniqueID field in the Certificate is a User ID or RDP ID associated with any such User Role or with an RDP as may be identified in the third column of that table.

| **Remote Party Role** | **Party** | **User Role or RDP** | **DCC Live Systems definition paragraph** |
|---|---|---|---|
| root | The DCC | [Not applicable] | (d) |
| recovery | The DCC | [Not applicable] | (f) |
| transitionalCoS | The DCC | [Not applicable] | (c) |
| wanProvider | The DCC | [Not applicable] | (a) |
| accessControlBroker | The DCC | [Not applicable] | (a) or (b) (as provided for in Section L3.18A) |
| issuingAuthority | The DCC | [Not applicable] | (d) |

| | | | |
|---|---|---|---|
| networkOperator | A Network Party | Either:<br>(a) Electricity Distributor; or<br>(b) Gas Transporter. | [Not applicable] |
| supplier | A Supplier Party | Either:<br>(a) Import Supplier; or<br>(b) Gas Supplier. | [Not applicable] |
| other | An RDP or any Party other than the DCC | Either:<br>Other User;<br>Registered Supplier Agent;<br>Registration Data Provider; or<br>Export Supplier. | [Not applicable] |
| pPPXmlSign | The DCC | [Not Applicable] | (g) |
| pPRDPFileSign | The DCC | [Not Applicable] | (g) |
| s1SPxmlSigning | The DCC | [Not Applicable] | (h) |
| xmlSign | An RDP or any Party other than the DCC | Either:<br>Import Supplier;<br>Gas Supplier;<br>Electricity Distributor;<br>Gas Transporter;<br>Other User;<br>Registered Supplier Agent;<br>Registration Data Provider; or<br>Export Supplier. | [Not applicable] |
| commissioningPartyFileSigning | The DCC | [Not Applicable] | [Only relevant during SMETS1 Migration] |
| requestingPartyFileSigning | The DCC | [Not Applicable] | [Only relevant during SMETS1 Migration] |
| s1SPMigrationSigning | The DCC | [Not Applicable] | [Only relevant during SMETS1 Migration] |
| commissioningPartyXmlSigning | The DCC | [Not Applicable] | [Only relevant during SMETS1 Migration] |
| loadController | None | None | [Not applicable] |
| cSSProvider | The DCC | [Not Applicable] | (j) |
| coSPartyXmlSign | The DCC | [Not Applicable] | (c) |
| dSPXmlSign | The DCC | [Not Applicable] | (a) |
| aCBXmlSign | The DCC | [Not Applicable] | (b) |
| wANProviderXmlSign | The DCC | [Not Applicable] | (a) |

## Add Section L17 as follows:

### L17 Interactions with CSS

L17.1 The DCC shall use a Private Key associated with a Public Key that is contained within an Organisation Certificate to Digitally Sign any communication sent pursuant to Section E2.19.

## Amend Annex A to Section L as follows:

### Annex A to Section L

Table 1: Remote Party Roles and associated Remote Party Role Codes in addition to those specified in the GB Companion Specification

| Remote Party Role | Remote Party Role Code |
|---|---|
| pPPXmlSign | 128 |
| pPRDPFileSign | 129 |
| s1SPxmlSigning | 126 |
| commissioningPartyFileSigning | 132 |
| requestingPartyFileSigning | 131 |
| s1SPMigrationSigning | 130 |
| commissioningPartyXmlSigning | 133 |
| cSSProvider | 134 |
| xmlSign | 135 |
| coSPartyXmlSign | 136 |
| dSPXmlSign | 137 |
| aCBXmlSign | 138 |
| wANProviderXmlSign | 139 |

# Section P ‘Production Proving’

These changes have been redlined against Section P version 7.0.

## Amend Section P1 as follows:

### P1. PRODUCTION PROVING

### Purpose

P1.1 The purpose of Production Proving is to provide assurance on the operation of the DCC Total System.

### Overview

P1.2 The DCC may, in its capacity as the Production Proving Function and subject to this Section P, to the extent reasonably necessary for the purposes of Production Proving:

(a) act as if it is a User (in different User Roles) to send Service Requests;

(b) act as if it is a User (in different User Roles) to receive Service Responses and Alerts in relation to Production Proving Devices (as if it was an Eligible User);

(c) act as if it is a User (in different User Roles) to access the Self Service Interface; and

(d) act as if it is ~~a Registration~~the CSS ~~Data~~ Provider in respect of Production Proving Registration Data.

### Production Proving Devices

P1.3 The Production Proving Function is only entitled to send a Service Request or Signed Pre-Command to the DCC that will result in communication with a Device where that Device is a Production Proving Device.

P1.4 A "**Production Proving Device**" is a (real) Device of a Device Model identified in the Central Products List, but one that has been procured by the DCC for the purposes of Production Proving.

P1.5 The Production Proving Function may send a Service Request requesting that the DCC adds a Production Proving Device to the Smart Metering Inventory (to be listed with an SMI Status of 'pending'), and the DCC shall add the Production Proving Device to the Smart Metering Inventory provided that the Production Proving Device is of a Device Model that is identified in the Central Products List.

P1.6 The Production Proving Function may install and Commission Production Proving Devices in order to create Smart Metering Systems, but those Production Proving Devices (and Smart Metering Systems) cannot be ones that record the supply of gas, or import or export of electricity, to or from a Premises for the purposes of settlement under the Energy Codes.

P1.7 The DCC shall not allow Production Proving Devices to be linked in the Smart Metering Inventory to (real) MPANs or MPRNs.

### Production Proving MPXNs

P1.8 Given the limitation set out in Section P1.7, the Production Proving Function is entitled to generate dummy MPANs and dummy MPRNs (collectively, "**Production Proving MPXNs**") for the purposes of Production Proving. The DCC may record these Production Proving MPXNs in the Smart Metering Inventory and link them to Production Proving Devices for the purposes of recording the Commissioning of Production Proving Devices. The DCC shall publish on the DCC Website the range of values which the DCC uses for Production Proving MPXNs.

P1.9 The Production Proving Function shall ensure that the Production Proving MPXNs are different from any and all MPANs and MPRNs, including that the data values of each Production Proving MPXN are outside the range that may in the future be used in an MPAN or MPRN.

P1.10 The DCC shall ensure that each Production Proving MPXN is only linked in the Smart Metering Inventory to a Production Proving Device (and not any other Device).

### Production Proving Registration Data

P1.11 The Production Proving Function may generate dummy Registration Data ("**Production Proving Registration Data**") for the purposes of Production Proving.

P1.12 The Production Proving Function shall ensure that the data fields in the Production Proving Registration Data by which Parties and other market participants are identified all contain data values which are different from the values used in the Registration Data to identify Parties and other market participants, including that the data values are outside the range that may in the future be used to identify Parties and other market participants.

P1.13 The Production Proving Function shall be entitled to send the Production Proving Registration Data to the DCC in accordance with Section E (Registration Data) acting as if the Production Proving Function was ~~a Registration Data~~the CSS Provider.

### Excluded Service Requests

P1.14 The Production Proving Function may not submit the following Service Requests (or send Signed Pre-Commands that relate to the following Service Requests):

(a) Update Security Credentials (KRP) (SRV 6.15);

(b) Request Handover Of DCC Controlled Device (SRV 6.21); or

(c) Update Security Credentials (CoS) (SRV 6.23).

### Testing

P1.15 The DCC shall, before it undertakes any or all of the activities set out in Section P1.2, successfully complete reasonable and appropriate testing of the Systems to be used as the Production Proving System.

P1.16 Prior to sending a Service Request to the DCC, the Production Proving Function must have successfully completed testing equivalent to User Entry Process Tests in the relevant User Role in which it wishes to act in sending that Service Request.

P1.17 ~~Prior to sending Production Proving Registration Data to the DCC, the Production Proving Function must have successfully completed testing equivalent to RDP Entry Process Tests.~~Not used.

## General Standards

P1.18 Where the DCC undertakes Production Proving, it shall do so in accordance with Good Industry Practice, and in a manner that does not adversely affect the provision of the Services.

## Production Proving IDs

P1.19 The Panel shall, where requested by the DCC, issue one or more Party Signifiers ~~and/or RDP Signifier~~ to the DCC for the purposes of identifying the DCC when acting as if it was a User or ~~an RDP~~a CSS Provider in its capacity as the Production Proving Function, and the Production Proving Function shall use these signifiers for such purpose.

P1.20 The Panel shall, where requested by the DCC, issue a new range of EUI-64 Compliant identifiers for use as DCC IDs by the DCC when acting as the Production Proving Function. This range must be outside the range of identifiers used by DCC as DCC IDs for any other DCC purpose under this Code.

P1.21 The DCC shall assign one or more DCC IDs for use only by the Production Proving Function.

P1.22 The DCC shall notify the Panel which DCC IDs are associated with which Production Proving Function Party Signifier~~, and which DCC IDs are associated with which Production Proving Function RDP Signifier~~.

P1.23 The Production Proving Function shall not use User IDs for the purpose of Production Proving.

## Security

P1.24 As the Production Proving Systems form part of the DCC Live Systems and the DCC Total System, the DCC shall ensure that it complies with the relevant requirements of Section G (Security) which apply as a consequence.

P1.25 The Production Proving Systems do not need to comply with the requirements of Section G (Security) which apply to User Systems or which apply to ~~RDP~~ the CSS Provider Systems (via Section E (Registration Data)); save that Section G6 (Anomaly Detection Thresholds: Obligations on the DCC and Users) shall apply to the Production Proving Function as if it was a User.

P1.26 For such purposes of Section G6 (Anomaly Detection Thresholds: Obligations on the DCC and Users), the Production Proving Function shall set Anomaly Detection Thresholds that have been approved by the Security Sub-Committee (and the DCC shall not process any communication from the Production Proving Function until such threshold values have been approved and set).

P1.27 In respect of the DCC's obligations under Section G6 (Anomaly Detection Thresholds: Obligations on the DCC and Users), not acting in the capacity of the Production Proving Function, the DCC shall set the Anomaly Detection Thresholds for the following Service Requests from the Production Proving Function to zero:

(a) Update Security Credentials (KRP) (SRV 6.15);

(b) Request Handover Of DCC Controlled Device (SRV 6.21); and

(c) Update Security Credentials (CoS) (SRV 6.23).

## Records and Reporting to the Security Sub-Committee

P1.28 The DCC shall:

(a) retain an audit log of the activities undertaken by the Production Proving Function for at least 6 years from the date on which the activity was undertaken;

(b) carry out post-event checks to confirm that no Service Requests or Signed Pre- Commands sent by the Production Proving Function resulted in communication with a Device which is not a Production Proving Device (or would have resulted in such communication had the DCC not rejected the message); and

(c) carry out post-event checks to ensure that the Production Proving Registration Data did not contain any (real) MPANs or MPRNs and did not use identifiers that are (or have been) used in the Registration Data to identify Parties and other market participants.

P1.29 The DCC shall, within 5 Working Days following the end of each month, provide a report to the Security Sub-Committee which summarises in respect of that month the matters referred to in Section P1.28.

## SMKI Services and DCCKI Services

P1.30 The Production Proving Function shall be entitled to receive SMKI Services and DCCKI Services under and in accordance with the relevant provisions of Section L (Smart Metering Key Infrastructure and DCC Key Infrastructure) and the SEC Subsidiary Documents applying pursuant to Section L as if it was a Party other than the DCC.~~:~~

~~(a) as if it was a Party other than the DCC; and~~
~~(b)~~(a) ~~as if it was an RDP.~~.

P1.31 The effect of Section P1.30 is to entitle the Production Proving Function to become an Authorised Subscriber, and to be an Eligible Subscriber in respect of those Device Certificates and Organisation Certificates for which the Production Proving Function is expressly stated to be eligible in Section L (Smart Metering Key Infrastructure and DCC Key Infrastructure).

P1.32 Before the Production Proving Function can apply to become an Authorised Subscriber or access the SMKI Repository, the Production Proving Function must have successfully completed testing equivalent to the SMKI and Repository Entry Process Tests.

P1.33 The Production Proving Function shall not submit any Certificate Signing Requests for a Device Certificate other than in relation to a Production Proving Device.

P1.34 The Production Proving Function shall not submit any Certificate Signing Request for an Organisation Certificate other than the one in relation to which it is identified as an Eligible Subscriber in Section L3 (The SMKI Services).

P1.35 The DCC is not required to implement controls within the DCA, an Issuing DCA or within the Registration Authority that limit the issuing of Device Certificates to the Production Proving Function in relation Production Proving Devices.

P1.36 The DCC shall ensure that no Public Key that is used by a Production Proving Device in relation to the Remote Party Role of either supplier or networkOperator is contained within any Certificate or other public key infrastructure certificate.

# Appendix X 'Registration Data Interface Specification'

These changes have been redlined against Appendix X version 2.0.

## Amend Appendix X as follows:

**DEFINITIONS**

In this document, except where the context otherwise requires:

- expressions defined in section A of the Code (Definitions and Interpretation) have the same meaning as is set out in that section; 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, Suspended or Withdrawn. |
| **DCC Status File** | means the file produced by DCC and transferred to each Network Party's Registration Data Provider detailing the DCC Service Flag of each MPAN or Supply Meter Point registered to that Network Party. |
| **Electricity Registration Data Provider** | means a Registration Data Provider appointed by an Electricity Network Party. |
| **Energy Market Data Specification** | means the Data Specification which forms part of the REC. |
| **FTP** | means file transfer protocol, a standard protocol for transmitting files between computers on a network. |
| **FTPS** | means FTP with Transport Layer Security. |
| **Gas Registration Data Provider** | means a Registration Data Provider appointed by a Gas Network Party. |
| **Internet Protocol (or IP)** | means the commonly used communications protocol enabling the delivery of data packets based on the IP addresses in the packet headers, used in establishing internet communications. |
| **Issuer** | has the meaning given to that term in the DCCKI Interface Design Specification. |
| **Network Address Translation** | means the standard methodology of remapping one IP address space into another by modifying network address information in Internet Protocol (IP) headers while they are in transit across a traffic routing device. |

**Policy Enforcement Point (or PEP)** a logical entity that enforces policies for admission control and policy decisions in response to a request for access. It is the logical boundary between the DCC Systems and connecting systems, namely User Systems and RDP Systems. The PEP ensures that:

a. the policies in the applicable Code of Connection relevant to the applicable party are being enforced;

b. there is appropriate separation of the DCC Systems from the connecting systems of the applicable party; and

c. all the connections to the User Systems, RDP Systems, or DCC Systems are compliant with the same applicable Code of Connection .

~~**Registration Data File**~~ ~~means the file or files containing Registration Data for one or more Network Parties, produced by (or on behalf of) each Network Party and transferred to the DCC detailing the Registration Data for that Network Party pursuant to Section E2 of the Code.~~

~~**Registration Data Refresh File**~~ ~~means the Registration Data File containing Registration Data for a subset or full set of MPANs or Supply Meter Points.~~

~~**Registration Data Update File**~~ ~~means the Registration Data File sent periodically that records changes to Registration Data.~~

**Response File** means a file produced whilst processing a DCC Status File. For each record in the file being processed, the Response File contains either an acknowledgement that the record has been processed successfully or in the case of a failure in processing the record, the validation errors found.

**Supported Version** means the latest version of the Energy Market Data Specification data flow that the DCC supports for use with the Registration Data Interface as listed and as updated from time to time on the Website.

**Transport Layer Security (or TLS)** means a protocol that provides for the privacy and integrity of data transferred between communicating applications and their users.

## 1. INTRODUCTION

### Document Purpose

1.1 Pursuant to Section E2~~.8~~ (Registration Data~~ Interface~~) of the Code, this document is the Registration Data Interface Specification.

## 2. REGISTRATION DATA INTERFACE

### Establishment of the REGIS logical connection

2.1 The DCC shall make the Registration Data Interface available on an Internet Protocol version 4 (IPv4) address range.

2.2 Each Registration Data Provider shall use Network Address Translation to remap their internal Internet Protocol addresses to the DCC provided Internet Protocol addresses at the Registration Data Provider's firewall prior to accessing the Registration Data Interface.

2.3 Each Registration Data Provider shall use Network Address Translation to remap incoming DCC traffic Internet Protocol addresses from the published Internet Protocol addresses at the Registration Data Provider's firewall to the Internet Protocol addresses the Registration Data Provider has reserved within their subnet.

2.4 The DCC shall specify a range of ports and the DCC and each Registration Data Provider shall configure these ports to be open for the FTPS connection.

**File Exchange Mechanism**

2.5 The Registration Data Interface shall utilise FTPS.

2.6 The DCC and each Registration Data Provider shall implement FTP, in a standard format conforming to the following internet standards as defined in the referenced Request for Comments (RFC) as published by the Internet Engineering Task Force (IETF) and the Internet Society:

(a) RFC 959 - FTP; and

(b) RFC 2228 – FTP security extensions.

2.7 The DCC and each Registration Data Provider shall secure the FTP session using TLS, in a standard format conforming to the following internet standards as defined in the referenced RFC as published by the IETF and the Internet Society:

(a) RFC 4217 - Securing FTP with TLS; and

(b) RFC 5246 - TLS version 1.2.

2.8 In accordance with RFC 4217:

(a) each Registration Data Provider shall populate the "USER command" (as defined in RFC 4217) with the RDP Signifier issued to it by the Panel, in lower case; and

(b) the DCC shall populate the "USER command" with the Party Signifier issued to it by the Panel, in lower case.

2.9 The DCC and each Registration Data Provider shall ensure the session Transport Layer Security is achieved utilising:

(a) the cipher suite TLS_RSA_WITH_AES_128_GCM_SHA256 as catalogued and further defined by the Internet Assigned Numbers Authority within the Cipher Suite Registry; and

(b) DCCKI Certificates for mutual authentication.

2.10 The DCC and each Registration Data Provider shall ensure that the FTPS session is routed via the DCC's Policy Enforcement Point and the Policy Enforcement Point used by the Registration Data Provider.

2.11 When sending a ~~Registration Data File or~~ DCC Status File, the DCC ~~and each Registration Data Provider~~ shall follow steps (a) to (d) below, and when receiving a ~~Registration Data File or~~ DCC Status File ~~the DCC and~~ each Registration Data Provider shall follow steps (e) to (k~~l~~) below:

(a) structure data files provided under Section~~s E2.1, E2.2 and~~ E2.4 of the Code, in accordance with the structures defined in clause~~s~~ 3.~~17~~9~~, 3.18, 3.19, 3.26, 3.28 and 3.29~~ of this document~~ and shall include a unique reference number in accordance with clauses 3.11 and 3.22~~;

(b) Digitally Sign the file in accordance with clause 2.1~~3~~2 of this document;

(c) connect to the recipient's FTPS server in accordance with clauses 2.7 to 2.9 of this document using a DCC Gateway Connection;

(d) initiate the transfer of the file to the relevant delivery directory on the recipient's FTPS server utilising FTP push mechanisms for all file exchanges;

(e) authenticate the source of the file through verifying that the file has been Digitally Signed in accordance with clause 2.1~~3~~2 of this document, and validate the file structure against the structure as defined in clause~~s 3.17, 3.18, 3.19, 3.26, 3.28 and~~ 3.~~2~~9 of this document;

(f) raise an Incident in accordance with the Incident Management Policy, where the recipient is unable to authenticate the file pursuant to clause 2.1~~7~~6 of this document;

(g) in the case of Electricity Registration Data Providers only, raise an Incident in accordance with the Incident Management Policy, where the Electricity Registration Data Provider is unable to confirm that the file conforms with clause 3.~~17~~9 of this document;

(h) in the case of Registration Data Providers only, generate a Response File as defined in clause ~~3.18(d)~~3.10(a) or ~~3.28(b)~~3.13(g) of this document, where the Registration Data Provider is unable to validate the file structure pursuant to clauses 3.~~19~~ 11 or 3.~~29~~ 14 of this document. The Registration Data Provider shall send the Response File to the DCC using the steps outlined in clauses 2.11(b) to (d) immediately above and on receipt of the Response File containing validation errors the DCC shall raise an Incident as defined in the Incident Management Policy;

~~(i) in the case of the DCC only, raise an Incident in accordance with the Incident Management Policy, where the DCC is unable to validate the file structure pursuant to clause 2.11(e) of this document;~~

~~(j)~~(i) process each record within the file and perform record level validation, where the Registration Data Provider or DCC is able to successfully authenticate and validate the file pursuant to clause 2.11(e) of this document;

~~(k)~~(j) in the case of Registration Data Providers only, generate a Response File as defined in clauses ~~3.18(d)~~3.10(a) and ~~3.28(b)~~3.13(g) of this document, where the Registration Data Provider is unable to successfully validate and process each record within the file pursuant to clause 2.11(i~~j~~) of this document. The Registration Data Provider shall send the Response File to the DCC using the steps outlined in clauses 2.11(b) to (d) and on receipt of the Response File containing validation errors the DCC shall raise an Incident in accordance with the Incident Management Policy; and

~~(l)~~(k) in the case of the DCC only, raise an Incident in accordance with the Incident Management Policy, where the DCC is unable to successfully validate and process each record within the file pursuant to clause 2.11(i~~j~~) of this document.

**Security Requirements**

~~2.12 The DCC shall allocate to each Registration Data Provider a separate directory within its FTPS server and permit access only to write files and obtain directory listings within their assigned directory, and not to read, modify or delete files.~~

~~2.13~~2.12 The DCC ~~and each Registration Data Provider~~ shall Digitally Sign each file sent via the Registration Data Interface with a Private Key~~; for the Registration Data Provider this Private Key shall be associated with an SMKI Organisation Certificate issued to the Registration Data Provider~~.

~~2.14~~2.13 The DCC ~~and each Registration Data Provider~~ shall ensure that the Digital Signature shall:

a) use, as the digital signature technique, Elliptic Curve Digital Signature Algorithm (ECDSA) (as specified in Federal Information Processing Standards Publications (FIPS PUB) 186-4) in combination with the curve P-256 (as specified in FIPS PUB 186-4 at Section D.1.2.3) and SHA-256 as the hash function;

b) be applied to the entirety of the file including header and trailer; and

c) be converted to Base64 and appended within the file itself to the trailer with a preceding "," separator.

~~2.15~~2.14 Prior to Digitally Signing each file, the DCC ~~and each Registration Data Provider~~ shall append to the trailer of the file the Issuer, which shall be URL encoded (as specified in the IETF RFC 2253), and serial number of the SMKI Organisation Certificate with preceding "," separators.

~~2.16~~2.15 ~~The DCC and e~~Each Registration Data Provider may use the organisation identifier in the header of the file and the Issuer and serial number in the trailer of the file to retrieve the appropriate public key.

~~2.17~~2.16 ~~The DCC and e~~Each Registration Data Provider shall Check Cryptographic Protection on a file using ECDSA (as specified in FIPS PUB 186-4) in combination with the curve P-256 (as specified in FIPS PUB 186-4 at Section D.1.2.3) and SHA-256 as the hash function, and Confirm Validity of the Certificate used to Check Cryptographic Protection.

~~2.18~~2.17 ~~The DCC and e~~Each Registration Data Provider shall ensure that the Digital Signature calculation shall:

(a) be performed on the entire file including header and trailer except the Digital Signature and preceding field separator appended to the trailer;

(b) ensure that all line termination characters read from the file, except any termination characters in the trailer, shall be normalised to 0x0A; and

(c) exclude any line termination characters in the trailer.

~~2.19~~2.18 Prior to verifying the Digital Signature, ~~the DCC and~~ each Registration Data Provider shall ensure that all line termination characters in the file, except the line termination characters in the trailer, shall be normalised to 0x0A.

**Interface Error Handling**

*Data files not being received when expected*

~~2.20~~2.19 Identification of an Anomalous Event:

~~(a) the DCC shall perform a check to ensure that the Registration Data Update Files being sent by the Registration Data Provider are consistent with the schedules as described in Section E2.5 (Frequency of Data Exchanges); and~~

~~(b)~~(a) in the event of the DCC or a Registration Data Provider identifying an exception to the agreed schedules, either organisation may raise an Incident in accordance with the Incident Management Policy.

~~2.21~~2.20 Connection & Transfer Failures:

(a) in the event of connection failures or file transfer failures ~~between the~~from the DCC to a Registration Data Provider ~~and the DCC~~, ~~the originating organisation~~the DCC shall attempt to reconnect and/or resend the file on 3 further occasions at 5 minute intervals; and

~~(b)~~ if the DCC cannot establish a connection with the Registration Data Provider after such number of retries, the DCC shall raise an Incident in accordance with the Incident Management Policy.~~; or~~

~~(c)~~(b) ~~if the Registration Data Provider fails to establish a connection with the DCC after such number of retries, the Registration Data Provider shall first confirm that the issue does not exist within their own environment and once this has been completed they may raise an Incident in accordance with the Incident Management Policy.~~

~~2.22~~2.21 Authentication Failure:

~~(a)~~ In the event of a transport authentication failure where the DCC is trying to send a DCC Status File to a Registration Data Provider, a transport authentication failure will result in no connection or transmission of Registration Data. In such circumstances, the DCC shall raise an Incident in accordance with the Incident Management Policy~~; or~~

~~(b)~~(a) ~~In the event of a transport authentication failure where a Registration Data Provider is trying to send a file to the DCC, a transport authentication failure will result in no connection or transmission of Registration Data. In such circumstances the Registration Data Provider shall raise an Incident in accordance with the Incident Management Policy.~~.

*Data files not conforming to the Registration Interface Specification*

~~2.23~~2.22 Identification of an Anomalous Event:

(a) The ~~DCC or~~ Registration Data Provider shall perform a check of the conformity of files against the agreed standards set out in clause 3 of this Registration Data Interface Specification; or

(b) In the event of either the DCC or a Registration Data Provider being in receipt of a non-conforming file ~~the respective organisation~~it shall raise an Incident in accordance with the Incident Management Policy.

~~2.24~~2.23 Validation Failure:

~~(a) where a validation failure is identified as a result of a Registration Data Provider file that has been sent to the DCC, the DCC shall raise an Incident in accordance with the Incident Management Policy; or~~

~~(b)~~(a) where a validation failure is identified as a result of a DCC file that has been sent to the Registration Data Provider, the Registration Data Provider shall raise an Incident in accordance with the Incident Management Policy.

~~2.25~~2.24 Other Circumstances:

(a) in the event of an Incident arising that is not covered by clauses 2.~~20~~ 19 to 2.~~24~~ 23 above, a Registration Data Provider shall review its business processes; and

(b) following compliance with clause ~~2.24 2.24(a)~~2.23(a) above, and in the event a Registration Data Provider has reasonable grounds to expect the issue to reside within the DCC, the Registration Data Provider shall raise an Incident in accordance with the Incident Management Policy.

*Notification of Delays*

~~2.26 In the event that a Registration Data Provider has a planned or unplanned delay to a Registration Data File transfer, the Registration Data Provider shall raise an Incident in accordance with the Incident Management Policy.~~

~~2.27~~2.25 In the event that the DCC has a planned or unplanned delay to a DCC Status File transfer, the DCC shall raise an Incident in accordance with the Incident Management Policy.

## 3. INTERFACE FILES

### General Obligations

3.1 The DCC shall maintain a separate unique reference number for each Network Party that it shall apply to all files corresponding to that Network Party that it sends through the Registration Data Interface to that Network Party's Registration Data Provider.

3.2 In the event that a file is suspected of being lost, each Registration Data Provider may raise an Incident in accordance with the Incident Management Policy.

3.3 Each Electricity Registration Data Provider shall, pursuant to clause 2.11(i~~j~~), reject a record with a DCC Service Flag 'effective from date' for a Smart Metering System that is earlier than the DCC Service Flag 'effective from date' previously provided by the DCC for that Smart Metering System.

3.4 Each Gas Registration Data Provider shall detect duplicate files and where detected shall not process duplicate files.

3.5 Each Gas Registration Data Provider shall process files in the order they are received.

3.6 Each Registration Data Provider and the DCC shall not use file compression on files transferred through the Registration Data Interface.

~~3.7 The DCC shall maintain a minimum of 24 months of the required historic Registration Data within DCC Systems.~~

~~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~~3.7 The DCC shall provide any DCC Status Files utilising the FTPS connection or via an alternative means as agreed between the DCC and the Gas Registration Data Provider or Electricity Registration Data Provider to whom the file is being sent, (provided that any such alternative means must incorporate the use of security controls that are at least as robust as those that apply to the FTPS connection) .

**Electricity Registration Data File Structure and Data Formats**

~~3.11 Each Electricity Registration Data Provider shall maintain a unique reference number for each Electricity Network Party that it shall apply to all files corresponding to that Electricity Network Party that it sends through the Registration Data Interface.~~

~~3.12 Each Electricity Registration Data Provider shall provide Registration Data Update Files in accordance with the schedule outlined in the Registration Data Interface Code of Connection irrespective of whether there are Registration Data updates to convey. Where there are no Registration Data updates, each Electricity Registration Data Provider shall provide a Registration Data Update File containing the standard header, trailer and unique sequence number record and no further data records.~~

~~3.13~~3.8 The DCC ~~and each Electricity Registration Data Provider~~ shall use variable length delimited file format for ~~exchanging~~ sending files, which meet the following requirements:

(a) fields shall be separated with "|" (ASCII 124) characters

(b) only use ASCII characters;

(c) not exceed the field lengths shown in the flow definitions referenced in clause 3.~~18~~ 9 of this document;

(d) values shall not be padded (with leading zeroes or trailing spaces) where less than the maximum field length;

(e) fields shall not be enclosed in double quotes;

(f) no characters shall be entered into fields that are intended to be blank; and

(g) records shall be terminated with a line feed (ASCII 10) character.

~~3.14 Each Electricity Registration Data Provider:~~

~~(a) shall provide a Registration Data Refresh File containing a subset of Registration Data where the DCC so requests in accordance with Section E2.7(b) (Frequency of Registration Data Exchange) of the Code;~~

~~(b) may provide an unsolicited Registration Data Refresh File, which shall not be considered an Anomalous Event, containing a subset of Registration Data; and~~

~~(c) where both Registration Data Refresh Files under clauses 3.14(a) and 3.14(b) are to be provided on the same day, the Registration Data Provider shall provide one Registration Data Refresh File to meet these combined requirements. The time by which these files need to be sent is set out in the Registration Data Interface Code of Connection.~~

~~3.15 Each Electricity Registration Data Provider shall employ a file naming convention that ensures that each of the files it sends through the Registration Data Interface has a unique name.~~

~~3.16 For electricity Registration Data Files, the DCC shall employ a file naming convention that ensures that each file sent through the Registration Data Interface has a unique name, using the following items separated by the underscore character, giving the overall naming layout: DCCO_D0123_123456 where:~~

~~(a) 'DCCO' is the organisation identifier (as defined in the Energy Market Data Specification);~~

~~(b) 'D0123' is the flow reference (as defined in the Energy Market Data Specification); and~~

~~(c) '123456' is a unique reference number (unique within DCC files for each Electricity Network Party).~~

~~3.17~~3.9 ~~Each Electricity Registration Data Provider and~~The DCC shall ensure that all files contain header and trailer records that conform to the formats as specified below:

(a) File Header

| Data Item | Format | Optionality | Comment |
|---|---|---|---|
| Group Header | CHAR(3) | Mandatory | 'ZHV' |
| File Identifier | CHAR(10) | Mandatory | File identifier - unique within market participant |
| Data flow and Version Number | CHAR(8) | Mandatory | Dxxxxnnn Consists of 5 char data flow reference followed by 3 char flow version number - where 'n' has a range of 0-9 e.g. 001, 105.... |
| From Market Participant Role Code | CHAR(1) | Mandatory | e.g. Registration systems have value P |
| From Market Participant Id | CHAR(4) | Mandatory | e.g. DCC has value DCCO |
| To Market Participant Role Code | CHAR(1) | Mandatory | e.g. DCC has value Z |
| To Market Participant Id | CHAR(4) | Mandatory | e.g. DCC has value DCCO |

| | | | |
|---|---|---|---|
| File creation timestamp | CHAR(14) | Mandatory | DATETIME (GMT) DCC is using UTC<br>Formatted:<br>YYYYMMDDHHMMSS |
| Sending Application Id | CHAR(5) | Optional | Application identifier. For possible future use |
| Receiving Application Id | CHAR(5) | Optional | Application identifier. For possible future use |
| Broadcast | CHAR(1) | Optional | For possible future use. |
| Test data flag | CHAR(4) | Optional | Indicates whether or not this file contains test data.<br>All operational (non-test) files shall contain the value OPER |

(b) File Trailer

| **Data Item** | **Format** | **Optionality** | **Comment** |
|---|---|---|---|
| Group Name | CHAR(3) | Mandatory | 'ZPT' |
| File identifier | CHAR(10) | Mandatory | File identifier - unique within market participant |
| Total Group Count | INT (10) | Mandatory | Total number of groups in file excluding header/trailer |
| Checksum | INT (10) | Optional | Checksum |
| Flow count | INT (8) | Mandatory | Number of flow instances excluding file header/trailer |
| File completion timestamp | CHAR(14) | Optional | DATETIME (GMT) DCC is using UTC<br>Formatted: YYYYMMDDHHMMSS |

~~3.18~~3.10 Each Electricity Registration Data Provider shall provide the following files, which shall conform to the latest Supported Version of the specified data flow structures as defined in the Energy Market Data Specification:

~~(a) Initial upload and full Registration Data Refresh File~~

~~To provide the DCC with an initial population of Registration Data and any subsequent full Registration Data refresh, each Electricity Registration Data Provider shall send a Registration Data Refresh File as specified in the Energy Market Data Specification D0353 data flow;~~

~~(b) Registration Data Update File~~

~~To notify the DCC of any changes to relevant Registration Data, each Electricity Registration Data Provider shall send a Registration Data Update File as specified in the Energy Market Data Specification D0348 data flow.~~

~~(c) Registration Data Refresh File - Partial refresh~~

~~To provide the DCC with a partial refresh of Registration Data, each Electricity Registration Data Provider shall send a Registration Data Refresh File as specified in the Energy Market Data Specification D0349 data flow;~~

~~(d)~~(a) Response File - DCC Service Flag update rejections

To notify the DCC of any data records rejected during processing of a DCC Status File due to validation errors, each Electricity Registration Data Provider shall send a Response File as specified in the Energy Market Data Specification D0351 data flow; and

~~(e)~~(b) Response File - DCC Service Flag update acknowledgement

To notify the DCC of successful processing of the DCC Status File, each Electricity Registration Data Provider shall send a Response File as specified in the Energy Market Data Specification D0172 data flow.

~~3.19~~3.11 The DCC shall provide the following files to each Electricity Registration Data Provider conforming to the data flow structures as defined in the Energy Market Data Specification:

(a) DCC Status File

To notify Electricity Network Parties of DCC Service Flag updates and the identity of the person that the DCC believes to be registered in relation to an MPAN as set out in Section E2.4 of the Code, the DCC shall send a DCC Status File as specified in the Energy Market Data Specification D0350 data flow.

~~3.20 Clauses 3.18(a), 3.18(b) and 3.18(c) constitute the Registration Data that is to be provided by Electricity Registration Data Providers to the DCC under Section E2.1 of the Code.~~

~~3.21~~3.12 Clause ~~3.19~~3.11 constitutes the data that is to be provided by the DCC to Registration Data Providers under Section E2.4 (a) of the Code.

**Gas Registration Data File Structure and Data Formats**

~~3.22 Each Gas Registration Data Provider shall maintain a unique reference number that it shall apply to each file it sends through the Registration Data Interface. Each file (with the exception of the multiple file confirmation file as defined in clause 3.28(c) of this document) shall include this unique reference number within the file header, taken from a monotonically increasing number generator. The DCC shall check this unique reference number in order to detect duplicate, missing or out of sequence files.~~

~~3.23~~3.13 The DCC ~~and each Gas Registration Data Provider~~ shall use comma separated file format for ~~exchanging~~ sending files to Registration Data Providers of Gas Transporters, and each shall ensure that all of the files that it sends meet the following requirements:

(a) fields shall be comma-separated;

(b) only use ASCII characters;

(c) do not exceed the field lengths shown below at clause 3.28 of this document and exclude any opening and closing double quotation marks or comma separators;

(d) values shall not be padded where less than the maximum field length;

(e) text fields shall be enclosed with opening and closing double quotation marks, but no quotation marks shall be used in date and numeric fields; and

(f) blank fields shall not contain characters other than opening and closing double quotation marks for text fields.

~~3.24~~3.14 Each Gas Registration Data Provider shall employ the file naming convention described below ~~in clauses (a) to (e)~~, ensuring that each file sent through the DCC Gateway Connection has a unique name. Within the names shown in clauses (a) ~~to~~ and (b~~e~~) below: 'PN' indicates that the files are production (will be 'TN' for test); nnnnnn is ~~be~~ the sequence number of the file in question; and xxx is the file type (ERR, FRJ or DXR) as detailed in clause 3.~~30~~16:

~~(a) Registration Data Update File:~~
~~XOS01.PNnnnnnn.XDO~~

~~(b) Registration Data Refresh File also used for initial population:~~
~~XOS02.PNnnnnnn.XDO~~

~~(c)~~(a) Daily DCC Status Files:
DCC01.PNnnnnnn.DXI

~~(d)~~(b) Response Files from Daily DCC Status File processing will be:
XOS01.PNnnnnnn.xxx

~~(e) Multiple file confirmation file where Registration Data has been split into multiple Registration Data Files:~~
~~XOS02.PNnnnnnn.TOK~~

~~3.25 In the circumstance where Registration Data Files need to be split into multiple files due to size limitations; each Gas Registration Data Provider shall additionally provide a multiple file confirmation file confirming the number of files within the set as defined in clause 3.28(c) of this document and with the file naming convention defined in clause 3.24(e) of this document.~~

~~3.26 Each Gas Registration Data Provider shall ensure that all files (with the exception of the multiple file confirmation file as defined in clause 3.28(c) of this document) contain header and trailer records that conform to the formats as detailed below:~~

~~(a) File Header~~

| ~~**Field Name**~~ | ~~**Type**~~ | ~~**Length**~~ | ~~**Description**~~ |
|---|---|---|---|
| ~~Transaction Type~~ | ~~Text~~ | ~~3~~ | ~~Value: A00~~ |
| ~~Organisation Id~~ | ~~Numeric~~ | ~~10~~ | ~~An reference which uniquely identifies the sending organisation~~<br>~~For example: DCC is 10005989~~ |

<table>
<tr><td>~~File Type~~</td><td>~~Text~~</td><td>~~3~~</td><td>~~An application specific code used to identify the structure and the usage of the file.~~<br>~~The allowable values are:~~<table><tr><td>XDO</td><td>Registration Data File</td></tr><tr><td>ERR</td><td>Response File - record level validation failure</td></tr><tr><td>FRJ</td><td>Response File - file level validation failure</td></tr><tr><td>DXI</td><td>DCC Status File</td></tr><tr><td>DXR</td><td>Response File - DCC Service Flag update response</td></tr></table></td></tr>
<tr><td>~~Creation Date~~</td><td>~~Date~~</td><td>~~8~~</td><td>~~The date on which the file was generated.~~<br>~~Format : YYYYMMDD~~</td></tr>
<tr><td>~~Creation Time~~</td><td>~~Text~~</td><td>~~8~~</td><td>~~The time (UTC) at which the file was generated (within the Creation Date)~~<br>~~Format : HHMMSS~~</td></tr>
<tr><td>~~Generation Number~~</td><td>~~Numeric~~</td><td>~~6~~</td><td>~~A sequence number which represents an issue of a file from the Registration Data Provider or DCC (indicated by the organisation id). Each file sent either from the Registration Data Provider to DCC or from DCC to the Registration Data Provider will have a unique consecutively increasing number.~~</td></tr>
</table>

~~(b) File Trailer~~

| ~~**Field Name**~~ | ~~**Type**~~ | ~~**Length**~~ | ~~**Description**~~ |
|---|---|---|---|
| ~~Transaction Type~~ | ~~Text~~ | ~~3~~ | ~~Value: Z99~~ |
| ~~Record Count~~ | ~~Numeric~~ | ~~10~~ | ~~The number of detail records contained within the file. This should not include the standard header and the standard trailer but should include any file specific headers if specified for this file i.e. only A00 and Z99 records are excluded.~~ |

~~3.27 Each Gas Registration Data Provider shall provide Registration Data Update Files to the schedule outlined in the Registration Data Interface Code of Connection irrespective of whether there are Registration Data updates to convey. Where there are no updates to provide the Registration Data Update File will contain the standard header, file sequence number and trailer and no data records.~~

~~3.28 Each Gas Registration Data Provider shall provide files to the DCC conforming to the following data flow structures:~~

~~(a) Registration Data Update Files~~

~~Registration Data updates shall be contained within a single file type (Ref XDO) and shall consist of up to 3 different types of data record per update as detailed below.~~

~~Where Registration Data needs to be split into multiple Registration Data Update Files due to size limitations, the data for a specific MPRN shall not be split between files.~~

~~(i) Data notifications (Ref E47, including data items for the Supply Meter Point such as address, postcode & UPRN)~~

| ~~**Field Name**~~ | ~~**Optionality**~~ | ~~**Type**~~ | ~~**Length**~~ | ~~**Description**~~ | ~~**Code reference**~~ |
|---|---|---|---|---|---|
| ~~Transaction Type~~ | ~~Mandatory~~ | ~~Text~~ | ~~3~~ | ~~Value: E47~~ | ~~Not applicable~~ |
| ~~Meter Point Reference (MPRN)~~ | ~~Mandatory~~ | ~~Number~~ | ~~10~~ | ~~A unique identifier for the point at which a meter is, has been or will be connected to the gas network.~~ | ~~Section E2.2 (c)~~ |
| ~~MPRN Status~~ | ~~Mandatory~~ | ~~Text~~ | ~~2~~ | ~~The current status of the operability of the meter.~~ | ~~Section E2.2 (d)~~ |
| ~~Source Registration Id~~ | ~~Mandatory~~ | ~~Text~~ | ~~3~~ | ~~Unique ID to identify the GT or iGT which has sent the data.~~ | ~~Not applicable~~ |
| ~~Meter Point Address~~ | ~~Optional~~ | ~~Text~~ | ~~250~~ | ~~Standard PAF format address for the Supply Meter Point. This field will be a concatenated form of the elements of the Supply Meter Point address available. The address will be separated within the text delimiters (double quotation marks) by commas. The address will be represented in a consistent manner in the following order:~~<br>~~Plot Number,~~<br>~~Building Number,~~<br>~~Sub Building Name,~~<br>~~Building Name,~~<br>~~Principal Street,~~<br>~~DependentLocalityPost Town.~~<br>~~If no address field data has been provided, the field will be blank denoted as ",,,,,,"~~ | ~~Section E2.2 (g)~~ |
| ~~Meter Point Postcode~~ | ~~Optional~~ | ~~Text~~ | ~~9~~ | ~~Standard PAF post code as defined in the PAF digest. The postcode will comprise the concatenated outcode and incode, separated by a space.~~ | ~~Section E2.2 (g)~~ |
| ~~Market Sector Flag~~ | ~~Optional~~ | ~~Text~~ | ~~1~~ | ~~A code that specifies that the site is used for Domestic or Industrial purposes.~~<br>~~The allowable values are:~~ | ~~Section E2.2 (h)~~ |

|  |  |  |  |  |  |
|---|---|---|---|---|---|
|  |  |  |  | ~~D – Domestic or I – Industrial.~~ |  |
| ~~Unique Property Reference Number~~ | ~~Optional~~ | ~~Text~~ | ~~12~~ | ~~A unique property reference number. It is a unique reference number that can be linked to further address information that is collated and provided by the Ordnance Survey Group.~~ | ~~Section E2.2 (g)~~ |

~~(ii) Organisation Notifications (Ref. E48, including details of the various organisations associated with the MPRN such as Gas Supplier, Meter Asset Manager and Gas Transporter).~~

| ~~**Field Name**~~ | ~~**Optionality**~~ | ~~**Type**~~ | ~~**Length**~~ | ~~**Description**~~ | ~~**SEC reference**~~ |
|---|---|---|---|---|---|
| ~~Transaction Type~~ | ~~Mandatory~~ | ~~Text~~ | ~~3~~ | ~~Value: E48~~ | ~~Not applicable~~ |
| ~~Organisation Type~~ | ~~Mandatory~~ | ~~Text~~ | ~~3~~ | ~~A three character short code denoting the role performed by the Organisation being notified as being effective at the Supply Meter Point denoted in the parent record.~~<br>~~The allowable values are:~~<br>~~SUP – Gas Supplier;~~<br>~~MAM – Meter Asset Manager;~~<br>~~NWO – Network Operator (Gas Transporter).~~ | ~~Section E2.2 (f)~~ |
| ~~Organisation Identifier~~ | ~~Mandatory~~ | ~~Text~~ | ~~3~~ | ~~A three character short code which is assigned by the Gas Transporter to denote the identity of the Organisation being notified as being effective at the Supply Meter Point denoted in the parent record.~~ | ~~Section E2.2 (f)~~ |
| ~~Organisation Effective From Date~~ | ~~Mandatory~~ | ~~Date~~ | ~~8~~ | ~~The date from which the Organisation was effective from or appointed to the Supply Meter Point denoted in the parent record.~~<br>~~Format : YYYYMMDD~~ | ~~Section E2.2 (f)~~ |
| ~~Organisation Effective To Date~~ | ~~Optional~~ | ~~Date~~ | ~~8~~ | ~~Organisation's Effective To Date.~~<br>~~Format : YYYYMMDD~~<br>~~N.B. Where the date is '00010101', this will be treated as Null~~<br>~~This will not be provided for Meter Asset Manager and Network Operator.~~ | ~~Section E2.2 (f)~~ |

~~(iii) Organisation Deletions (Ref. E49, including details of the various organisations previously associated with the MPRN which are now to be deleted). This record type is used to delete future dated organisations which will no longer come into effect due to other data changes. For example where a new Meter Asset Manager is due to be associated with an MPRN, but a change of supplier occurs before the effective date and the supplier assigns their own Meter Asset Manager.~~

| ~~**Field Name**~~ | ~~**Optionality**~~ | ~~**Type**~~ | ~~**Length**~~ | ~~**Description**~~ | ~~**SEC reference**~~ |
|---|---|---|---|---|---|
| ~~Transaction Type~~ | ~~Mandatory~~ | ~~Text~~ | ~~3~~ | ~~Value: E49~~ | ~~Not applicable~~ |
| ~~Organisation Type~~ | ~~Mandatory~~ | ~~Text~~ | ~~3~~ | ~~A three character short code denoting the role performed by the Organisation being notified as being effective at the Supply Meter Point denoted in the parent record.~~<br>~~The allowable values are:~~<br>~~SUP – Gas Supplier;~~<br>~~MAM – Meter Asset Manager;~~<br>~~NWO – Network Operator (Gas Transporter).~~ | ~~Section E2.2 (f)~~ |
| ~~Organisation Identifier~~ | ~~Mandatory~~ | ~~Text~~ | ~~3~~ | ~~A three character short code which is assigned by the Gas Transporter to denote the identity of the Organisation being notified as being effective at the Supply Meter Point denoted in the parent record.~~ | ~~Section E2.2 (f)~~ |
| ~~Organisation Effective From Date~~ | ~~Mandatory~~ | ~~Date~~ | ~~8~~ | ~~The date from which the Organisation was effective from or appointed to the Supply Meter Point denoted in the parent record.~~<br>~~Format : YYYYMMDD~~ | ~~Section E2.2 (f)~~ |
| ~~Organisation Effective To Date~~ | ~~Optional~~ | ~~Date~~ | ~~8~~ | ~~Organisation's Effective To Date.~~<br>~~Format : YYYYMMDD~~<br>~~NB Where the date is '00010101', this will be treated as Null~~ | |

~~(b)~~(c) Response File - DCC Service Flag update responses

Following the processing of the DCC Status File (file format described in clause 3.15~~29~~(a) of this document) each Gas Registration Data Provider shall provide a Response File indicating whether each of the DCC Service Flag update records (record reference 'E45') was accepted or rejected. For each E45 record in the incoming "DXI" DCC Status File there will be a corresponding E46 record (as described immediately below) in the "DXR" Response File. If the E45 record is processed successfully, the outcome code in the E46 record will be "AC" and if unsuccessful the outcome code is "RJ".

Where the outcome is “RJ” the rejection reason will be notified to the DCC through an S72 record or records directly following the E46.

(i) The format of an E46 record is as follows:

| Field Name | Optionality | Type | Length | Description |
|---|---|---|---|---|
| Transaction Type | Mandatory | Text | 3 | Value: E46 |
| Outcome Code | Mandatory | Text | 2 | Details whether the request has been accepted or rejected.<br>AC – Accepted<br>RJ – Rejected. |
| Meter Point Reference | Mandatory | Number | 10 | |
| DCC Service Flag | Mandatory | Text | 1 | Service flag provided by the DCC.<br>The allowable values are:<br>A Active<br>S Suspended<br>W Withdrawn |
| DCC Service Effective From Date | Mandatory | Date | 8 | The date the DCC Service Flag (provided above) is effective from.<br>Format : YYYYMMDD |

(ii) The format of an S72 record is as follows:

| Field Name | Optionality | Type | Length | Description |
|---|---|---|---|---|
| Transaction Type | Mandatory | Text | 3 | Value: S72 |
| Rejection Code | Mandatory | Text | 8 | The unique reference number identifying the reason for the validation failure.<br>One of the following two values: ‘MPO00001’<br>Supply Meter Point does not exist<br>‘DCC00001’<br>DCC Service Flag value is not recognised |

~~(c) Multiple file confirmation file~~

~~Where Registration Data needs to be split into multiple files due to size limitations, each Gas Registration Data Provider shall provide an additional file confirming the number of files within the set.~~

| ~~Field Name~~ | ~~Optionality~~ | ~~Type~~ | ~~Length~~ | ~~Description~~ |
|---|---|---|---|---|
| ~~File Name~~ | ~~Mandatory~~ | ~~Text~~ | ~~18~~ | |
| ~~Record Count~~ | ~~Mandatory~~ | ~~Number~~ | ~~10~~ | ~~The number of detail records contained within the file. This should not include the standard header and the standard trailer but should include any file specific headers if specified for this file i.e. only A00 and Z99 records are excluded.~~ |

~~3.29~~3.15 The DCC shall provide files to each Gas Registration Data Provider conforming to the following data flow structure:

(a) DCC Status File

To notify each Gas Registration Data Provider of DCC Service Flag updates the DCC shall send a single DCC Status File (Ref DXI) that shall consist of a single data record per update (Ref. E45). The format of an E45 record is as follows:

| Field Name | Optionality | Type | Length | Description | SEC reference |
|---|---|---|---|---|---|
| Transaction Type | Mandatory | Text | 3 | Value: E45 | Not applicable |
| Meter Point Reference | Mandatory | Number | 10 | | Section E2.4 (b) |
| DCC Service Flag | Mandatory | Text | 1 | Service flag provided by the DCC.<br>The allowable values are:<br>A Active<br>S Suspended<br>W Withdrawn | Section E2.4 (b) |
| DCC Service Effective From Date | Mandatory | Date | 8 | The date the DCC Service Flag (provided above) is effective from.<br>Format : YYYYMMDD | Section E2.4 (b) |

~~3.30~~3.16 Each Gas Registration Data Provider shall create and send the Response Files as defined in clause 3.~~30~~ 16 (a) and (b) below, in response to failures in validation of the DCC Status File. On receipt of the Response File DCC shall raise an Incident as defined in the Data Incident Management Policy.

(a) Record level format failure Response File

To record any record level format validation errors found in processing the DCC Status File, the Gas Registration Data Provider shall create a Response File with header and trailer as defined in clause

3.~~26~~ 14 of this document and one or more record level error records as detailed below. The file name will be as defined in clause ~~3.24(d)~~3.14(b) of this document with suffix ‘ERR’.

| Field Name | Optionality | Type | Length | Description |
|---|---|---|---|---|
| Transaction Type | Mandatory | Text | 3 | Value: E01 |
| Rejection Code | Mandatory | Text | 8 | The unique reference number identifying the reason for the validation failure as defined in the Error Code under clause 3.30(c) |
| File Reference | Mandatory | Number | 10 | The unique reference number of the file that was received and processed. |
| Rejection Description | Mandatory | Text | 250 | Description of the error found and which record/field it occurred as defined in the Rejection Reason under clause 3.30(c). |

(b) Response File - File level rejection

To record any file level format validation errors found in processing the DCC Status File, the Registration Data Provider shall create a Response File with header and trailer as defined in clause 3.26 of this document and the file name will be as defined in clause 3.24(d) of this document with suffix ‘FRJ’. File level validation failures will be contained within a single file and will consist of 2 different types of data record per file – Rejected File (record reference S71) and Rejection Details (record reference S72). There will be one S71 record followed by one or more S72 records.

(i) The format of an S71 record is as follows:

| Field Name | Optionality | Type | Length | Description |
|---|---|---|---|---|
| Transaction Type | Mandatory | Text | 3 | Value: S71 |
| File Reference | Mandatory | Text | 30 | The unique reference number of the file that was received and processed. |

(ii) The format of an S72 record is as follows:

| Field Name | Optionality | Type | Length | Description |
|---|---|---|---|---|
| Transaction Type | Mandatory | Text | 3 | Value: S72 |
| Rejection Code | Mandatory | Text | 8 | The unique reference number identifying the reason for the validation failure as defined in the Error Code under clause 3.30(d) |

(c) Record level - Error codes

| **Error Code** | |
|---|---|
| CSV00010 | Transaction type not recognized - <*Record identifier*> |
| CSV00011 | Invalid character - <*Record identifier*>, <*Field number*> |
| CSV00012 | Invalid numeric field , <*Record identifier*>, <*Field number*> |
| CSV00013 | Premature end of record - <*Record identifier*> |
| CSV00014 | Invalid record termination - <*Record identifier*> |
| CSV00015 | Invalid text field - <*Record identifier*>, <*Field number*> |
| CSV00019 | Record too short - <*Record identifier*> |
| CSV00020 | Mandatory field expected - <*Record identifier*>, <*Field number*> |
| CSV00021 | Invalid Date/Time field - <*Record identifier*>, <*Field number*> |
| CHK00036 | Mandatory record not supplied - <*Record identifier*> |

(d) File level - Error codes

| | |
|---|---|
| FIL00013 | Organisation ID on header cannot be found |
| FIL00014 | Organisation ID on the header does not match the sender's ID |
| FIL00015 | File type on the header is not the same as that in file name |
| FIL00016 | Generation number on the header is not the same as that in file name |
| FIL00017 | A file has previously been received & processed with this generation number |
| FIL00018 | A count of detail records in the file does not match that held on the trailer |
| FIL00019 | Invalid record type found |

# Appendix Y ‘Registration Data Interface Code of Connection’

These changes have been redlined against Appendix Y version 2.0.

## Amend Appendix Y as follows:

**DEFINITIONS**

In this document, except where the context otherwise requires:

- expressions defined in Section A of the Code (Definitions and Interpretation) have the same meaning as is set out in that Section;
- the expressions in the left hand column below shall have the meanings given to them in the right hand column below; and
- any expressions not defined here or in Section A of the Code have the meaning given to them in the Registration Data Interface Specification.

| | |
|---|---|
| **Security Patch** | means a software change intended to address a particular vulnerability or weakness in the security of a system. |

**1. REGISTRATION DATA INTERFACE CODE OF CONNECTION**

1.1 These provisions apply to the DCC and any Registration Data Provider seeking to ~~send and~~ receive communications via the Registration Data Interface.
General Obligations

1.2 The DCC and each Registration Data Provider shall inform each other of the contact details of one or more persons working for their respective organisations for the purposes of managing arrangements associated with the use of the Registration Data Interface. The following information shall be provided in relation to each such person (and subsequently kept up to date by the providing organisation):

(a) contact name;

(b) contact email;

(c) contact telephone number; and

(d) contact address.

and any other contact details as may be reasonably required by the DCC or the Registration Data Provider from time to time.

**Restrictions on the use of DCC Gateway Connections**

1.3 ~~Each Registration Data Provider shall only send Registration Data over a DCC Gateway Connection, except where an alternative means of transfer has been agreed pursuant to clause 3.8 or 3.9 of the Registration Data Interface Specification.~~ The DCC shall use ~~that~~ a~~same~~ DCC Gateway Connection for the purpose of sending data to the Registration Data Provider pursuant to Section E2 of the Code, except where an alternative means of transfer has been agreed pursuant to clause 3.~~10~~ 7 of the Registration Data Interface Specification.

### Establishment of Transport Layer Security

1.4 The DCC and each Registration Data Provider:

(a) shall establish a TLS session to secure the transport layer connection to the Registration Data Provider's FTPS server and the DCC's FTPS server respectively and shall do so in accordance with the Registration Data Interface Specification;

(b) shall use a DCCKI Infrastructure Certificate to establish the TLS session; and

(c) in the case of a Registration Data Provider only, may obtain a DCCKI Infrastructure Certificate in accordance with the DCCKI RAPP.

### ~~Registration Data~~DCC Status Files

~~1.5 Each Gas Registration Data Provider shall produce a Registration Data Update File showing changes to the Registration Data that occurred during the preceding day, provided that where no such changes have occurred, the Registration Data Update File shall record zero changes.~~

~~1.6 Each Electricity Registration Data Provider shall produce a Registration Data Update File showing changes to the Registration Data that occurred during the preceding Working Day, provided that where no such changes have occurred, the Registration Data Update File shall record zero changes.~~

~~1.7 Pursuant to clause 1.5 of this document, each Gas Registration Data Provider shall send each Registration Data Update File to the DCC via the Registration Data Interface by 06:00 hours on the following day to which the data in the file relates.~~

~~1.8 Pursuant to clause 1.6 of this document, each Electricity Registration Data Provider shall send the Registration Data Update File to the DCC via the Registration Data Interface by 06:00 hours on the following Working Day to which the data in the file relates.~~

~~1.9~~1.5 The DCC shall produce a DCC Status File showing the changes to the DCC Service Flag for each MPAN or Supply Meter Point that occurred since the last update, provided that where no such changes have occurred, the DCC Status File shall record zero changes.

~~1.10~~1.6 The DCC shall send a DCC Status File by 18:00 hours every day. In the case of Gas Smart Metering Systems, the DCC shall send one DCC Status File per Registration Data Provider. In the case of Electricity Smart Metering Systems, the DCC shall send one DCC Status File per Electricity Network Party.

~~1.11 Each Registration Data Provider shall, prior to sending its first set of Registration Data to the DCC, provide to the DCC a size estimate of a file containing a full Registration Data Refresh File.~~

~~1.12 Each Registration Data Provider shall inform the DCC in advance of sending Registration Data Files where the number of records requires the Registration Data Provider to split the data into multiple files due to file size restrictions within the Registration Data Provider's systems.~~

~~1.13 The DCC shall monitor use of the Registration Data Interfaces and ensure that adequate capacity is provided for each Registration Data Provider to enable the fulfilment of its obligations to provide Registration Data to the DCC under Section E of the Code.~~

### ~~Registration Data Refreshes~~

~~1.14 The means by which the DCC shall request a re-submission or a refresh of a Registration Data File is for the DCC to contact the Registration Data Provider.~~

~~1.15 When requesting a full or partial file refresh or re-submission of a Registration Data File, the DCC shall take reasonable steps to contact the Registration Data Provider prior to 16:00 on the day of the request.~~

~~1.16 Pursuant to Section E2.12 of the Code, having been requested to refresh or resubmit a file in accordance with clause 1.14 of this document a Registration Data Provider shall send the file to the DCC via the Registration Data Interface, in accordance with the Registration Data Interface Specification and the timings set out in clauses 1.17 or 1.18 below. On receipt of the file, the DCC shall upload the file as detailed in the Registration Data Interface Specification.~~

~~1.17 Electricity Registration Data Provider timetable for file provision:~~

| ~~Type~~ | ~~Action~~ | ~~Time~~ |
|---|---|---|
| ~~Full Refresh~~ | ~~Full Refresh of the Registration Data to the DCC~~ | ~~As per Section E2.7(a) of the Code~~ |
| ~~Partial Refresh~~ | ~~A Partial Refresh is a submission of a subset of the Registration Data to the DCC~~ | ~~The file(s) shall be submitted within the timelines directed in the REC~~ |
| ~~File re-submission~~ | ~~Re-submission of a file that is not received or is corrupt~~ | ~~Within 1 Working Day of the request for re-submission having been made pursuant to clause 1.14 of this document~~ |

~~Table 1 - Timetable – Electricity~~

~~1.18 Gas Registration Data Provider timetable for file provision:~~

| ~~Type~~ | ~~Action~~ | ~~Time~~ |
|---|---|---|
| ~~Full Refresh~~ | ~~Full Refresh of the Registration Data to the DCC~~ | ~~As per Section E2.7(a) of the Code~~ |
| ~~Partial Refresh~~ | ~~A Partial Refresh is a submission of a subset of the Registration Data to the DCC~~ | ~~Within the shorter of three Working Days or four days~~ |
| ~~File re-submission~~ | ~~Re-submission of a file that is not received or is corrupt~~ | ~~Within 1 Working Day of the request for re-submission having been made pursuant to clause 1.14 of this document~~ |

~~Table 2 - Timetable – Gas~~

### Technical Infrastructure

~~1.19~~1.7 Each Registration Data Provider shall provide and configure its own FTPS servers for use in ~~sending and~~ receipt of ~~Registration Data~~data from the DCC as set out in Section E2.4~~,~~ and shall be responsible for operation and maintenance of its FTPS platform used to receive files from the DCC.

~~1.20~~1.8 Each Registration Data Provider and the DCC shall inform each other of information relating to its FTPS servers that is reasonably required by the DCC and each Registration Data Provider in relation to any DCC Gateway Connection that it is using to access the Registration Data Interface.

~~1.21 Each Registration Data Provider shall provide the DCC with reasonable advance notice via the Service Desk, of any expected outages which may affect that Registration Data Provider's ability to send Registration Data to the DCC.~~

~~1.22~~1.9 The DCC shall ensure that the URLs and/or the IP addresses of the Registration Data Interface remain constant.

**Security Obligations**

~~1.23~~1.10 Each Registration Data Provider shall test the installation of Security Patches to be applied to its RDP Systems prior to their application.

~~1.24~~1.11 Prior to using the Registration Data Interface, each Registration Data Provider shall provide a report to the DCC that details the following:

(a) the scope of its RDP Systems;

(b) the number of connections between its RDP Systems and any System that does not form part of the RDP Systems; and

(c) the means by which the Registration Data Provider has achieved Separation between its RDP Systems and each other System to which they connect.

and;
thereafter, the Registration Data Provider shall ensure that the DCC is provided with a revised report whenever there is a change to the information in its previous report.

~~1.25~~1.12 Where, based upon the report provided by the Registration Data Provider in clause 1.~~24~~11 of this document the DCC considers that the Registration Data Provider has not adequately Separated its RDP Systems from other systems to which those RDP Systems connect, then to the extent that the failure to adequately Separate poses a threat of Compromise to DCC's Systems, the DCC shall notify the Registration Data Provider, the relevant Network Party, and the Panel and provide an associated explanation.

# Appendix AG ‘Incident Management Policy’

These changes have been redlined against Appendix AG version 3.0.

## Amend Section 1.2 as follows:

### 1.2. Background

1.2.1 The subject matter of this document is closely related to that of the Incident Management aspects of the Registration Data Interface Specification. In order to ensure an integrated solution to managing Incidents, certain common aspects of Incident Management are set out in this document and cross-referred to in the Registration Data Interface Specification.

1.2.2 The ~~timetable for Registration Data refreshes is set out in the Registration Data Interface Code of Connection and the~~ Registration Data Incident types are set out in the Registration Data Interface Specification.

1.2.3 Error conditions and how they should be handled are covered in Clause 4, the Error Handling Strategy.

## Amend Section 2.1 as follows:

## 2. INCIDENT MANAGEMENT

### 2.1. Pre-requisites to Raising an Incident

**DCC**

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

2.1.2 ~~Pursuant to Section E2.13, prior to the DCC raising an Incident regarding the provision of Registration Data by a Registration Data Provider, the DCC shall take all reasonable steps to confirm that the issue does not reside within the DCC System or processes.~~Not used.

**Incident Parties other than Registration Data Providers**

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

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

(a) where appropriate, confirm that the issue does not reside within the HAN, or the Smart Meter, or other Devices which the Incident Party is responsible for operating;

(b) confirm that the issue does not reside within the Incident Party’s own systems and processes;

(c) follow the guidance set out in the self-help material made available by the DCC, including checking for Known Errors and the application of any workarounds specified; and

(d) where the party is a User and to the extent that this is possible, use the SSI or submit a Service Request to resolve the Incident in accordance with Section H9.2.

2.1.4 In the event that the activities in clause 2.1.3 have been completed and an Incident is to be raised with the DCC, where it has access to the Self-Service Interface, the Incident Party shall check on the Self Service Interface to establish whether an Incident has already been raised or a Service Alert issued for this issue and:

(a) in the event that the Incident Party can reasonably determine that an Incident or Service Alert for this issue exists, the Incident Party shall notify the Service Desk who shall register the Incident Party as an Interested Party within the Incident Management Log;

(b) in the event that the Incident Party cannot identify an existing Incident or Service Alert they shall progress to clause 2.2 to raise an Incident.

### Registration Data Provider

2.1.5 Prior to raising an Incident regarding the provision of data ~~to and~~ by the DCC, the Registration Data Provider shall take all reasonable steps to confirm that the issue does not reside within the Registration Data Provider's systems and processes.

## Amend Section 5.2 as follows:

## 5.2 Business Continuity and Disaster Recovery Procedures

### Disaster Recovery

5.2.1 Pursuant to the requirements of Section H10.9:

(a) the DCC shall implement the measures in the table below under 'DCC Mitigation' to reduce the likelihood of the Disaster occurring and limit the impact in the event that a Disaster has occurred;

(b) in the event of a Disaster, the DCC shall follow the actions in the table below detailed under 'DCC Recovery Action'; and

(c) Incident Parties may experience the impact set out in the table below under 'Incident Party Impact' and shall follow the actions as detailed under 'Incident Party Actions on failure, failover or failback'.

| Disaster ID | DCC Disaster Impact | DCC Mitigation | DCC Recovery Action | Incident Party Impact | Incident Party Actions on failure, failover or failback | Applicable to SMETS1 or SMETS2+? |
|---|---|---|---|---|---|---|
| D1(a) | The DCC loses the primary data centre provided pursuant to the (data services) contract | The DCC shall provide primary and secondary data centres providing data services for the DCC Live Systems, with | The DCC shall do one of the following: | Incident Parties may experience a loss of all Services on failover to the secondary data centre and on failback to the primary | 1. When requested by the DCC, Incident Parties shall suspend submission of Service Requests and Signed Pre-Commands | SMETS2+ |

| | | | | | | |
|---|---|---|---|---|---|---|
| | referred to in paragraph 1.2(a) of Schedule 1 of the DCC Licence. | a resilient server configuration in the primary data centre with an active-passive configuration between data centres.<br>All configurations and data are backed up and backups are stored offsite. There are resilient network links to the data centres providing communication services. | a. fail over to the secondary data centre; or<br>b. recover Services at the primary data centre. | data centre, with the exception of some Testing Services which operate from the secondary data centre. | until notified that Services have been restored.<br>2. Upon restoration of impacted Services, Incident Parties may recommence submission of Service Requests and Signed Pre-Commands (including submitting any that have failed).<br>3. When requested by the DCC, the Incident Party shall take each of the actions identified in column 6, of rows D5, D8, D9, D10, D11 and D16 of this table 3 and B6, B7 and B12 of table 4 below, as relevant, when DCC fails over from or fails back to the primary data centre. | |
| D1(b) | The DCC loses the primary data centre provided pursuant to the SMETS1 Data Services contract(s). | The DCC shall provide primary and secondary data centres in order to provide data services for the DCC Live Systems, with a resilient server configuration in the primary data centre with an active-passive configuration between data centres.<br>All configurations and data are backed up and backups are stored offsite. There are resilient network links to the data centres providing communication services. | The DCC shall do one of the following:<br>a. fail over to the secondary data centre; or<br>b. recover Services at the primary data centre. | Incident Parties may experience a partial loss of SMETS1 Services on failover to the secondary data centre and on failback to the primary data centre. | Upon restoration of impacted Services, Incident Parties may recommence submission of SMETS1 Service Requests (including submitting any that have failed). | SMETS1 |
| D2 | The DCC loses the secondary data centre provided pursuant to the (data services) contract referred to in paragraph 1.2(a) of Schedule 1 of the DCC Licence. | The DCC shall provide the ability to deliver Testing Services from either the secondary or primary data centres.<br>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:<br>a. recover Services at the primary data centre; or<br>b. recover Services at the secondary data centre. | Incident Parties will experience a loss of some Testing Services.<br>Incident Parties may experience a loss of some data within Testing Services. | 1. When requested by the DCC, Incident Parties shall suspend the use of Testing Services until notified that Services have been restored.<br>2. Upon Services restoration, Incident Parties may resubmit failed test messages. | SMETS2+ |
| D3(a) | The DCC loses both the primary and secondary data centres provided pursuant to the (data services) contract referred to in paragraph 1.2(a) of Schedule 1 of the DCC Licence. | The DCC shall ensure that all configurations & data are backed up & backups are stored offsite. | The DCC shall do one or more of the following:<br>a. recover Services at the primary data centre;<br>b. recover Services at the secondary data centre;<br>c. restore Services to new infrastructure at an alternative data centre;<br>d. set up network links to the new data centre; | Incident Parties may experience a loss of all Services.<br>Incident Parties may experience a loss of some transactions.<br>Some information related to billing and Service Levels may be lost.<br>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.<br>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 | 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: | Incident Parties may experience a partial loss of all SMETS1 Services.<br>Incident Parties may experience a loss of some | Upon restoration of impacted Services, Incident Parties shall resubmit any that have failed SMETS1 Service Requests. | SMETS1 |

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

| | | | | | | |
|---|---|---|---|---|---|---|
| | | | | | 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.<br>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:<br>a. fail over to the secondary data centre; or<br>b. recover Services at the primary data centre. | Incident Parties would be unable to successfully send CoS Update Security Credentials Service Requests.<br>Incident Parties may experience a loss of all Services during the failover to the secondary data centre.<br>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:<br>• in respect of SMETS2+, the submission of Service Requests and Signed Pre-Commands; and<br>• in respect of SMETS1, the submission of SMETS1 Service Requests.<br>2. Upon restoration of impacted Services, Incident Parties may recommence submission (including submitting any that have failed) of:<br>• in respect of SMETS2+, Service Requests and Signed Pre-Commands; and<br>• in respect of SMETS1, SMETS1 Service Requests.<br>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:<br>a. recover connection at the primary data centre;<br>b. recover connection at the secondary data centre;<br>c. recover User connection. | Incident Parties will experience loss of connectivity to Services via the DCC User Gateway Connection. | 1. In the event of a Services interruption, when advised by the DCC, Incident Parties shall suspend submission via the DCC User Gateway Connection until Services are restored of:<br>• In respect of SMETS2+, Service Requests and Signed Pre-Commands; and<br>• in respect of SMETS1, SMETS1 Service Requests.<br>2. In the event of a Services interruption, when requested by the DCC, Incident Parties shall only submit Category 1 Incidents.<br>3. Upon restoration of impacted Services, Incident Parties may recommence submission (including submitting any that have failed) of:<br>• In respect of SMETS2+, Service Requests and Signed Pre-Commands; and | SMETS1 and SMETS2+ |

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

| | | | | | | | |
|---|---|---|---|---|---|---|---|
| D12 | Intentionally Blank | | | | | | |
| D13 | The DCC loses its primary data centre provided pursuant to the (SMKI) contract referred to in Schedule 1 of the DCC Licence. | The DCC shall provide instances of the SMKI service infrastructure at primary & secondary SMKI data centres in an active-passive configuration with full data replication between sites and resilient network links to the Data Service Provider.<br>The DCC shall backup all SMKI configurations & data and shall store backups offsite. | The DCC shall do one of the following:<br>a. fail over to the secondary data centre; or<br>b. recover Services at the primary data centre. | Incident Parties would be unable to request new Organisational or Device Certificates during failure, failover or failback to the primary data centre. | 1. When requested by the DCC, Incident Parties shall suspend transmission of Certificate Signing Requests.<br>2. Upon restoration of impacted Services, Incident Parties may recommence submission of Certificate Signing Requests (including submitting any that have failed). | SMETS1 and SMETS2+ |
| D14 | The DCC loses both primary & secondary data centres provided pursuant to the (SMKI) contract referred to in Schedule 1 of the DCC Licence. | The DCC shall maintain full off-site configuration & data backups. | The DCC shall:<br>a. Restore failed services at one of the existing datacentres; or<br>b. restore failed Services to new infrastructure at an alternative data centre and shall then redirect network links to the alternate data centre. | Incident Parties may be unable to request new Organisational or Device Certificates. | When requested by the DCC, Incident Parties shall suspend submission of Certificate Signing Requests until Services have been restored.<br>Upon Services restoration, Incident Parties may resubmit failed Certificate Signing Requests. | SMETS12 and SMETS2+ |
| D15(a) | The DCC loses both primary data centres provided pursuant to the DCO (Dual Control Organisation) contract. | The DCC shall provide primary and secondary data centres in order to provide data services for the DCC Live Systems, with a resilient server configuration in the primary data centre with an active-passive configuration between data centres.<br>All configurations and data are backed up and backups are stored offsite. There are resilient network links to the data centres providing communication services. | The DCC shall do one of the following:<br>a. fail over to the secondary data centre; or<br>b. recover Services at the primary data centre. | Incident Parties may experience a partial loss of SMETS1 Services on failover to the secondary data centre and on failback to the primary data centre. | Upon restoration of impacted Services, Incident Parties may recommence submission of SMETS1 Service Requests (including submitting any that have failed). | SMETS1 |
| D15 (b) | The DCC loses both primary & secondary data centres provided pursuant to the (Dual Control Organisation) contract. | The DCC shall maintain full off-site configuration & data backups. | The DCC shall do one or more of the following:<br>recover Services at the primary data centre;<br>b. recover Services at the secondary data centre;<br>c. restore Services to new infrastructure at an alternative data centre; or<br>d. set up network links to the new data centre. | Incident Parties will experience a loss of all SMETS1 Services.<br>Incident Parties may experience a loss of some SMETS1 transactions to a particular S1SP.<br>On restart the DCC may impose systems-driven Restrictions on transaction volumes/types. | When requested by the DCC, Incident Parties shall suspend submission of all SMETS 1 Service Requests until Services have been restored.<br>Upon restoration of impacted Services, Incident Parties may recommence submission of SMETS1 Service Requests (including submitting any that have failed). | SMETS1 |
| D16 | A failure of a connection or interface between one or more Registration Data | There are resilient network links to the Registration Data Providers from both primary and secondary data centres. | The DCC shall do one or more of the following:<br>recover connection at the primary data centre; | There may be a delay in the ~~update of registration data on the DCC. This may cause some Service Requests to fail registration data checks even though the Party submitting them is an~~ | Upon service restoration, Incident Parties may resubmit failed Service Requests and/or SMETS1 Service Requests. | SMETS1 and SMETS2+ |

| | | | | | | |
|---|---|---|---|---|---|---|
| | Providers (RDP) and the DCC | | b. recover connection at the secondary data centre;<br>c. recover connection to the Registration Data Provider; or<br>d. Send ~~and receive~~ Registration update by alternative (secure) means. | ~~Eligible User~~issuing of DCC Status Files. | When requested by the DCC, RDPs shall ~~send and~~ receive updates by alternative (secure) means. | |
| D17 | The DCC loses a data centre provided pursuant to the (communications services) contract referred to in paragraph 1.2(b) of Schedule 1 of the DCC Licence. | The DCC shall provide primary & secondary sites for communication services data centres in an active-active configuration. All configurations & data are backed up and backups are stored offsite.<br>In the event of failure of one communications service data centre, Services would continue to be provided from the secondary data centre. | The DCC shall:<br>restore the provision of Impacted Services at the affected communications data centre; or<br>b. restore the provision of impacted Services at a new data centre. | There would be no impact on Incident Parties from a single communications service data centre failure.<br>Restoration of the existing data centre will not impact Incident Parties. | No action would be required from Incident Parties to resolve this Incident.<br>Restoration of the existing data centre will not require action from Incident Parties. | SMETS1 and SMETS2+ |
| D18 | The DCC loses both data centres provided pursuant to the (communications services) contract referred to in paragraph 1.2(b) of Schedule 1 of the DCC Licence. | The DCC shall maintain full off-site configuration & data backups. | The DCC shall:<br>restore impacted Services to new infrastructure at the affected location(s); or<br>b. restore services at an alternative data centre(s) | Incident Parties may be unable to send Commands to Devices or receive Responses and Device Alerts via the DCC and will experience loss of some Services. | 1. When requested by the DCC, Incident Parties shall suspend submission until notified that Services have been restored of:<br>• In respect of SMETS2+, Service Requests and Signed Pre-Commands; and<br>• in respect of SMETS1, SMETS1 Service Requests.<br>2. Incident Parties shall also comply with all reasonable DCC requests to assist with prioritising & phasing back transmission of Service Requests and/or SMETS1 Service Requests. | SMETS1 and SMETS2+ |
| D19 | The service provided pursuant to the contract referred to in paragraph 1.2(b) of Schedule 1 of the DCC Licence experiences multiple access node failure (Failure of a single access node would not be regarded as a DCC Disaster). | The DCC has significant, although not complete, overlap between access nodes.<br>The DCC shall ensure that access nodes are of a resilient design and that it has sufficient provision of mobile equipment and components spares to restore service within acceptable timescales. | The DCC shall:<br>deploy field maintenance and/or mobile equipment to restore Services. | Incident Parties may experience the failure of impacted Services directed to meters, Communications Hubs and Gas Proxy Functions in the affected area(s). | Upon Services restoration, Incident Parties may resubmit failed Service Requests and/or SMETS1 Service Requests. | SMETS1 and SMETS2+ |
| D20 | Communications Hub Product Recall | The DCC has more than one source for Communications Hubs.<br>Buffer stocks are held by the DCC and Communications Hub manufacturers. | The DCC shall:<br>a. determine the nature and extent of the problem; and<br>b. notify all Incident Parties of the extent of product recall required and effects on existing stocks and future supply. | This could result in Incident Parties diverting field staff to uninstall affected Communications Hubs, resulting in delays in installations.<br>It might also impact stocks and future supply. | Incident Parties shall provide reasonable assistance to the DCC in resolving issues. | SMETS2+ |

| | | | | | | |
|---|---|---|---|---|---|---|
| D21 | Loss of a site housing a DCC service function | The DCC shall have arrangements in place to resume all activity at an alternate location as part of its business continuity arrangements. | The DCC shall:<br>a. relocate the service function to the designated recovery site & shall restore service from there; or<br>b. recover services at existing site | Incident Parties may be unable to contact the affected service function until it has been recovered at an alternate location. | There is no action required from Incident Parties. | SMETS1 and SMETS2+ |
| D22 | Intentionally Blank | | | | | |

Table 3 – Disaster Recovery Procedures

# Appendix AL ‘SMETS1 Transition and Migration Approach Document’

These changes have been redlined against Appendix AL version 18.0.

## Amend Section 3.1(a) as follows:

## 3 Transitional Application of Sections of the Code

### Application of Section A (Definitions and Interpretation)

3.1 Whilst this TMAD remains in force, Section A (Definitions and Interpretation) of the Code shall apply as follows:

(a) the definition of “DCC Live Systems” shall be replaced with the following:

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

(a) (other than to the extent to which the activities fall within paragraph (b), (c), (f), (g), (h), (i), (j), ~~or~~ (k) or (l) below) processing (including Countersigning of SMETS1 Responses, SMETS1 Alerts and S1SP Alerts, but not Countersigning of SMETS1 Service Requests) Service Requests, Pre-Commands, Commands, Instructions, Service Responses and Alerts, holding or using Registration Data for the purposes of processing Service Requests and Signed Pre-Commands, and providing the Repository Service;

(b) ~~(other than to the extent to which the activity falls within paragraph (i) below)~~ Threshold Anomaly Detection (other than that carried out by a DCO) and (other than to the extent to which the activity falls within paragraph (d), (f), (g), (h), (i), (j), ~~or~~ (k) or (l) below) Cryptographic Processing relating to the generation and use of a Message Authentication Code and Countersigning

SMETS1 Service Requests;

(c) discharging the obligations placed on the DCC in its capacity as CoS Party;

(d) providing SMKI Services;

(e) the Self-Service Interface;

(f) discharging the DCC’s obligations under the SMKI Recovery Procedure;

(g) the Production Proving Systems;

(h) discharging the obligations of any SMETS1 Service Provider in its capacity as such;

(i) discharging the obligations of any DCO in its capacity as such;

~~(i)~~(j) discharging the obligations of the CSS Provider in its capacity as such;

~~(j)~~(k) discharging the obligations of any Requesting Party in its capacity as such; and

~~(k)~~(l) discharging the obligations of the Commissioning Party in its capacity as such.

(b) the definition of “DCC Individual Live System” shall be replaced with the following:

**DCC Individual Live System**

means, with regard to the DCC's duty to Separate parts of the DCC Total System, a part of the DCC Total System which is used:

(a) for one of the purposes specified in paragraphs (a) to (g), or (j) or paragraph (l~~k~~) of the definition of DCC Live Systems, where the part used for each such purpose shall be treated as an individual System distinct from:

(i) the part used for each other such purpose; and

(ii) any part used for a purpose specified in either paragraphs (h) to (k~~j~~) of the definition of DCC Live Systems; or

(b) by a SMETS1 Service Provider for the purpose specified in paragraph (h) of the definition of DCC Live Systems, where the part used by each SMETS1 Service Provider shall be treated as an individual System distinct from:

(i) the part used by each other SMETS1 Service Provider; and

(ii) any part used for a purpose specified in any of paragraphs (a) to (g), or paragraphs (i) to (l~~k~~), of the definition of DCC Live Systems; or

(c) by a DCO for the purpose specified in paragraph (i) of the definition of DCC Live Systems, where the part used by each DCO shall be treated as an individual System distinct from:

(i) the part used by each other DCO; and

(ii) any part used for a purpose specified in any of paragraphs (a) to (h) or paragraphs (j) ~~and~~ to (l~~k~~) of the definition of DCC Live Systems; or

(d) by a Requesting Party for the purpose specified in paragraph (~~j~~k) of the definition of DCC Live Systems, where the part used by each Requesting Party shall be treated as an individual System distinct from:

(i) the part used by each other Requesting Party; and

(ii) any part used for the purpose specified in any of paragraphs (a) to (~~i~~j) or paragraph (l~~k~~) of the definition of DCC Live Systems.

## Amend Section 3.1(e) as follows:

(e) the following definitions shall be added to Section A:

| | |
|---|---|
| Commissioning Party | Shall mean the DCC when performing the tasks ascribed to the Commissioning Party in this Code. |
| Commissioning Party Systems | That part of the DCC Total System used for the purposes referred to in sub-paragraph (l~~k~~) of the definition of DCC Live Systems. |
| DCC Migration Systems | Shall mean the Requesting Party Systems and the Commissioning Party Systems. |
| Migration | In relation to a SMETS1 Installation, or any Device comprising part of that SMETS1 Installation, the carrying out of each of the steps (where relevant to the point of failure) set out in Clauses 5 and 6 of the Transition and Migration Approach Document in relation to that SMETS1 Installation or Device; and the term "Migrate" shall be interpreted accordingly. |
| Migration Incident | Shall mean an Incident that relates to the Services provided pursuant to the Transition and Migration Approach Document. |
| Requesting Party | Shall mean, in relation to each of one or more Groups, the DCC when performing the tasks ascribed to the Requesting Party in this Code. |
| Requesting Party Systems | Shall mean those parts of the DCC Total System used when carrying out the role of a Requesting Party, provided that any SMETS1 SMSO's Systems from which information is provided to the Requesting Party for the purposes of populating the content of any Migration Common File, Migration Group File or Migration Group Encrypted File (each as defined in the Transition and Migration Approach Document) shall not be considered to form part of the Requesting Party Systems. |

| | |
|---|---|
| Smart Metering Inventory Systems | Shall mean that part of DCC Systems that is capable of adding to, modifying or removing any information held in the Smart Metering Inventory and any other part of DCC Systems that is not Separated from it. |
| SMETS1 Loss of System Availability | Shall mean a material loss of availability, other than for Maintenance purposes, of the DCC Migration Systems, or any of its individual components. |