Version: AL 7.0

APPENDIX AL

SMETS1 Transition and Migration Approach Document

1 Introduction and General Obligations

1.1 This Appendix is the Transition and Migration Approach Document (TMAD) developed by the DCC pursuant to Section N6 of the Code.

1.2 Where directed to do so by the Secretary of State from time to time, the DCC shall develop and consult upon a further draft or drafts of this TMAD and submit it to the Secretary of State in accordance with the process set out in Section N6.4 of the Code.

1.3 For the purposes of Section N6.8 (Expiry of Transition and Migration Approach Document) this TMAD will cease to apply on 31 December 2020 (or any such later date as the Secretary of State may direct following a consultation on a proposed alternative with the Parties and the Panel).

2 Defined Terms and Interpretations

Term	Meaning
Active Device	Shall mean an Active Meter or Active GPF as the context requires.
Active GPF	Shall mean the SMETS1 GPF that is associated with a SMETS1 GSME that is an Active Meter.
Active Meter	Shall mean, at the relevant point in time, a SMETS1 ESME or a SMETS1 GSME in relation to which, at that point in time, the Responsible Supplier has arrangements with a SMETS1 SMSO to provide the Responsible Supplier with services in relation to that SMETS1 ESME or SMETS1 GSME.
Authenticator	Shall be the DCC, the DCO, the Commissioning Party, a Supplier Party or the S1SP when undertaking the processing required by Table 5.9.
Authorised DCO SMETS1 Device Credentials	Shall mean the security related information required by the DCO for a SMETS1 Device which is provided to the DCO securely (and independently from the S1SP) and which the DCO is required to use to independently assure requests it receives from the S1SP in relation to the Device's installation or Migration.
Authorised S1SP SMETS1 Device Credentials	Shall mean the security related information required by the S1SP for a SMETS1 Device which is provided to the S1SP securely (and independently from the DCO) and which the S1SP is required to use in relation to the Device's installation or Migration.

Term	Meaning
Certificate ID	In relation to an Organisation Certificate, shall be the combination of serialNumber and Issuer X520 Common Name (with their Organisation Certificate Policy meanings) and so shall be a unique identifier for that Organisation Certificate. Thus, the identifier shall be the SMETS1 Migration Schema combination of the X509SerialNumber and X509IssuerName values. Where no Organisation Certificate is identified, it shall have the Null Certificate ID value.
CHF Identifier	Shall be the Device ID of the SMETS1 CHF associated with each SMETS1 Installation.
CHF Whitelist	In relation to a SMETS1 Installation, shall include the list of Device IDs, being IEEE media access control addresses, held on the SMETS1 CHF detailing the set of Devices which are currently authorised to communicate over the ZigBee network to which the CHF controls access. For clarity this list never includes Device IDs for a CHF or a GPF, and in the case of an ESME only includes the Device ID where that ESME communicates with the CHF using a ZigBee network. For clarity, the CHF Whitelist, for GroupIDs specified in Clauses 12, 13, 14, 15 and 16, includes, for each IEEE media access control address either (1) the UTC date-time at which the CHF last communicated with the identified Device or (2) an indication that the CHF has never communicated with the identified Device.
Commissioning Outcome File	Shall mean a file created by the Commissioning Party which complies with the requirements of Clause 6.3(d)(ii).
Commissioning Outcome File Counter	A counter of that name created and maintained pursuant to Table 5.7 to guard against replay of files processed pursuant to this TMAD.
Commissioning Party	See Clause 3.1(e).
Commissioning Party Systems	See Clause 3.1(e).
Commissioning Request	Shall mean a request from the Commissioning Party as set out in Table 6.3.
Common Validation Checks	Shall means those checks carried out pursuant to Clause 5.10.
Critical Network Operator ID	In relation to an Organisation Certificate identified by a specified Certificate ID, if it has a Remote Party Role of ‘networkOperator’ and a keyUsage of ‘digitalSignature’, the Critical Network Operator ID shall be the Entity Identifier of the subject of that Certificate (all with their Organisation Certificate Policy meanings). Otherwise, the Critical Network Operator ID shall be null.

Term	Meaning
Critical Supplier ID	In relation to an Organisation Certificate identified by a specified Certificate ID, if it has a Remote Party Role of 'supplier' and a keyUsage of 'digitalSignature', the Critical Supplier ID shall be the Entity Identifier of the subject of that Organisation Certificate (all with their Organisation Certificate Policy meanings). Otherwise, the Critical Supplier ID shall be null.
Daily Migration Demand	Shall have the meaning given in Clause 4.8.
DCC's Microsoft SharePoint	A web-based collaborative platform that DCC uses to securely share and exchange information with individual Parties.
DCC Migration Systems	Shall have the meaning given in Clause 3.1(e).
DCO Public Key	Shall mean a public key produced pursuant to Clause 5.4A.
DCO Required File Set	Shall mean the set of files specified in Clauses 12, 13, 14, 15 and 16 for the relevant GroupID.
DCO Viable Installations	Shall have the meaning ascribed to that term in Clause 5.19.
Dormant Meter	Shall mean, in relation to a SMETS1 SMSO, a SMETS1 ESME or a SMETS1 GSME that is installed in respect of an Energy Consumer's premises, that: i) the relevant SMETS1 SMSO is able to remotely communicate with via a SMETS1 CHF; and ii) is not an Active Meter.
Group	Shall mean the set of SMETS Installations identified by the same GroupID on the Group Device Model Combination List.
Group Device Model Combination List	Shall mean a list of Device Model Combinations that are entries on the SMETS1 Eligible Product Combinations list and form part of the same Group.
GroupID	Shall be the unique value used by the DCC to identify a Group within the Group Device Model Combination List.
Group Specific Requirements	Shall mean the set of requirements as specified in Clauses 12, 13, 14, 15 and 16 for the relevant GroupID.
IEEE	The Institute of Electrical and Electronics Engineers.

Term	Meaning
Indicative Migration Forecasts	In relation to a Supplier Party and a SMETS1 SMSO, shall mean the forecast number of all SMETS1 Installations that the Supplier Party is planning to include within a Migration Authorisation each day and the associated dates. This forecast shall be broken down by Electricity Network Party.
Installing Supplier	Means, in relation to a Device, the Supplier Party that installed, or arranged for the installation of, that Device.
Key Identifier	The SHA-1 hash of a Public Key that is used to identify that Public Key, where SHA-1 has the meaning specified in the US Government's Federal Information Processing Standards document 180-4.
Last EPCL Entry	Means, in respect of entries that include Secure SMSO Limited (company number 10611361), the entry on the list of SMETS1 Eligible Product Combinations which has been approved by the Secretary of State after which no other entries in respect of Secure SMSO Limited have been approved by the Secretary of State for a period of 12 months.
Migration	Shall have the meaning given in Clause 3.1(e).
Migration Authorisation	An authorisation given by the Responsible Supplier in relation to a SMETS1 Installation via the Migration Authorisation Mechanism to commence the Migration of a SMETS1 Installation, or an authorisation deemed to be given in accordance with Clause (a). Where there are two Responsible Suppliers for the Smart Metering Systems that together comprise the same SMETS1 Installation and they are Affiliates of one another, then any authorisation for the Migration of the SMETS1 Installation from the Responsible Supplier for the Electricity Smart Metering System shall, where the Migration Authorisation Mechanism also includes details of the Gas Smart Metering System, be deemed to constitute an authorisation for Migration of the SMETS1 Installation by the Responsible Supplier for the Gas Smart Metering System.
Migration Authorisation Mechanism	The mechanism of that name referred to in Clause 4.35.
Migration Common File	Shall mean a file created by a Requesting Party pursuant to Clause 5.8 that details information about SMETS1 Installations, along with the additional requirements for the relevant GroupID.
Migration Common File Counter	A counter of that name created and maintained pursuant to Table 5.7 to guard against replay of relevant files processed pursuant to this TMAD.

Term	Meaning
Migration Common Validation File	Shall mean a file created by the DCC pursuant to Clause 5.10(b) detailing, for a corresponding Migration Common File, which SMETS1 Installations have passed the Common Validation Checks and which have not. For those which have not, the file shall specify the validation failure. For clarity, any SMETS1 Installation which does not pass the Common Validation Checks shall not be further processed by the DCC in relation to the corresponding Migration Common File.
Migration Common Validation File Counter	A counter of that name created and maintained pursuant to Table 5.7 to guard against replay of relevant files processed pursuant to this TMAD.
Migration Demand Commitment	Shall have the meaning given in Clause 4.8(b).
Migration Error Handling and Retry Strategy	Shall have the meaning set out in Clause 8.8.
Migration Group Encrypted File	Shall mean a file created by a Requesting Party pursuant to Clause 5.12(g) which details a list of SMETS1 Installations which the Requesting Party wishes to Migrate, as identified by the CHF Identifier of each, along with the additional Group Specific Requirements for the relevant GroupID. For clarity, such files shall only be processed where they are specified as being required in Group Specific Requirements.
Migration Group Encrypted File Counter	A counter of that name created and maintained pursuant to Table 5.7 to guard against replay of relevant files processed pursuant to this TMAD.
Migration Group File	Shall mean a file created by a Requesting Party pursuant to Clause 5.12(f) which details a list of SMETS1 Installations which the Requesting Party wishes to Migrate as identified by the CHF Identifier of each, along with, where required for the Group identified by GroupID, any additional Group Specific Requirements for the relevant GroupID. For clarity, such files shall only be processed where they are specified as being required in the Group Specific Requirements.
Migration Group File Counter	A counter of that name created and maintained pursuant to Table 5.7 to guard against replay of relevant files processed pursuant to this TMAD.
Migration Header	In relation to a file created pursuant to this TMAD, the combination of the values in the RequestingPartyID and MCFCounter elements, each with the meaning set out in Clause 10.
Migration Incident	Shall have the meaning given in Clause 3.1(e).
Migration Reporting Regime	Shall have the meaning given in Clause 4.45.
Migration Scaling Methodology	Shall have the meaning given in Clause 4.11.

Term	Meaning
Migration Week	Means in relation to a SMETS1 SMSO, a period of seven days commencing on a Monday and within which DCC plans to Migrate one or more SMETS1 Installations that pertain to that SMETS1 SMSO. The first Migration Week for a SMETS1 SMSO shall commence on the first Monday following the day on which an entry for a combination of Device Models which lists that SMETS1 SMSO, as part of that entry, has been added to the SMETS1 Eligible Product Combinations.
Network Operator Certificate ID	The Certificate ID of an Organisation Certificate that has been Issued to a Network Party.
Non-Critical Network Operator ID	In relation to an Organisation Certificate identified by a specified Certificate ID, if it has a Remote Party Role of 'networkOperator' and a keyUsage of 'keyAgreement', the Non-Critical Network Operator ID shall be the Entity Identifier of the subject of that Certificate (all with their Organisation Certificate Policy meanings). Otherwise, the Non-Critical Network Operator ID shall be null.
Non-Critical Supplier ID	In relation to an Organisation Certificate identified by a specified Certificate ID, if it has a Remote Party Role of 'supplier' and a keyUsage of 'keyAgreement', the Non-Critical Supplier ID shall be the Entity Identifier of the subject of that Certificate (all with their Organisation Certificate Policy meanings). Otherwise, the Non-Critical Supplier ID shall be null.
Null Certificate ID	Shall be the Certificate ID used to mean that no Certificate is identified. The value of Null Certificate ID shall be the combination where `serialNumber` and Issuer X520 Common Name (with their Organisation Certificate Policy meanings) are '0' and 'NULL' respectively.
Plaintext	When used in relation to symmetric key encryption / decryption, shall have its GBCS meaning. When used in relation to public key encryption / decryption, shall mean the 'message M' with its IETF RFC-8017 meaning.
Recovery Time Objective	Shall be the targeted duration of time within which a system must be restored after a disaster (or disruption).
Recovery Point Objective	Shall be the targeted duration of time over which Data can be lost due to a Major Incident.
Relevant Device	Means an Active Meter in a SMETS1 Installation with which, prior to the UTRN Period, Secure SMSO Limited (company number 10611361) communicated on behalf of the Responsible Supplier.
Requested Installations	Shall have the meaning ascribed to that term in Clause 5.12.
Requesting Party	See Clause 3.1(e)

Term	Meaning
Requesting Party Systems	See Clause 3.1(e).
RP Decommissioning Date	Means, in relation to a Requesting Party, the decommissioning date identified in relation to that Requesting Party in the RP Decommissioning Timetable.
RP Decommissioning Timetable	The timetable of that name most recently approved by the Secretary of State pursuant to Clause 7.3.
Single Use Authorisation Code (SUA)	A one-time authorisation code used by Devices with GroupID = "DA" when cryptographically verifying Instruction.
S1SP Commissioning File	Shall mean a file created by the S1SP pursuant to Clause 5.27(c)(ii) which details whether, for the SMETS1 Installations in question, the S1SP successfully undertook the processing required of the S1SP and, if not fully successful, the issues arising in that processing.
S1SP Commissioning File Counter	A counter of that name created and maintained pursuant to Table 5.7 to guard against replay of files processed pursuant to this TMAD.
S1SP Required File Set	Shall mean the set of files specified for the relevant GroupID.
S1SP Viable Installations	Shall have the meaning set out in Clause 5.25.
SMETS1 CAD	Shall be a Device operating on a home area network created by a SMETS1 CHF, which is not a SMETS1 ESME, a SMETS1 GSME, a SMETS1 CHF, a SMETS1 GPF, a SMETS1 PPMID or a SMETS1 IHD.
SMETS1 Device Security Testing	means tests carried out by the DCC in accordance with the requirements of Clause 17.
SMETS1 Device Security Testing Completion Report	means the document of that name developed pursuant to Clause 17.11.
SMETS1 Device Security Testing Scope and Timetable Document	means the document of that name developed pursuant to Clause 17.3.
SMETS1 Installation	Means a SMETS1 CHF installed in respect of an Energy Consumer's premises, the SMETS1 GPF which is part of the same SMETS1 CH, the SMETS1 ESME with which the SMETS1 CHF can communicate, and the set of other Devices (if any) which are authorised to communicate over the HAN to which the CHF controls access. The set of other Devices within a SMETS1 Installation shall include at most one SMETS1 GSME, at most one SMETS1 PPMID, at most one SMETS1 IHD and at most one SMETS1 CAD.

Term	Meaning
SMETS1 Loss of System Availability	Shall have the meaning given in Clause 3.1(e).
SMETS1 Migration Interface	Shall be the technical interface, as specified at Clause 9, used for the exchange of files between the DCC and Supplier Parties pursuant to the requirements to exchange files in this TMAD.
SMETS1 Migration Schema	The XML SMETS1 Migration Schema included at Clause 10.
SUA Symmetric Key	A secret, symmetric key used by the DCO to authorise Critical Instructions (with its SMETS1 Supporting Requirements meaning), in relation to Devices with a GroupID = "DA".
Supplier Certificate ID	The Certificate ID of an Organisation Certificate that has been Issued to a Supplier Party.
Supplier Signifier	The Party Signifier of the Supplier Party identified by the Entity Identifier of the subject in the Organisation Certificate identified by any CriticalSupplierCertificateID in the Migration Common File. If any CriticalSupplierCertificateID in the Migration Common File is the Null Certificate ID, the value of the Supplier Signifier shall be the empty string.
UTRN Period	In relation to an ESME or a GSME that forms part of a SMETS1 Installation that is within the Group with a GroupID = "DA", a period that: (a) commences from the time at which the step in 3.14C(a) has been successfully passed in relation to that Device; and (b) has a duration that is 336 hours.

2.2 The XML elements listed in Table 10.1 are references to the parts of the SMETS1 Migration Schema and shall have the meaning given to them in the SMETS1 Migration Schema. Where such XML elements are referred to in this TMAD, then as the context requires, the reference shall be interpreted to be either to the element that is to be populated or to the information that is populated within that element for a particular file.

2.3 Additionally, where defined terms from specific parts of the Code are used, the relevant part of the Code is stated. Where no specific part of the Code is stated, a defined term shall have its Section A (Definitions and Interpretation) meaning.

2.4 Where this TMAD affords rights to, or imposes obligations on, a Party in relation to a Migration Week, then, until such time as an entry exists on the list of Eligible Product Combinations in respect of a particular SMSO, the term "Migration Week" in respect of that SMSO shall be interpreted as meaning each week that the Party reasonably anticipates will be a Migration Week (based on the milestones set out in the SMETS1 Services delivery plan produced pursuant to condition 13 of the DCC Licence).

3 Transitional Application of Sections of the Code

Application of Section A (Definitions and Interpretation)

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

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

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

(a) (other than to the extent to which the activities fall within paragraph (b), (c), (f), (g), (h), (i), (j) or (k) 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) below) Cryptographic Processing relating to the generation and use of a Message Authentication Code and Countersigning SMETS1 Service Requests;

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

(d) providing SMKI Services;

(e) the Self-Service Interface;

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

(g) the Production Proving Systems;

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

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

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

(k) 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 paragraph (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 (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 (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 (k) of the definition of DCC Live Systems; or

(d) by a Requesting Party for the purpose specified in paragraph (j) 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) or paragraph (k) of the definition of DCC Live Systems.

(c) the definition of "Planned Maintenance shall be replaced with the following:

Planned Maintenance	means, in respect of a month, Maintenance of the DCC Systems planned prior to the start of that month or, in the case of DCC Migration Systems, planned 10 Working Days prior to the start of the Maintenance, and which will disrupt, or poses a Material Risk of disruption to, provision of the Services (and, where it will disrupt, or poses a Material Risk of disruption to, the provision of the Services in relation to Devices associated with Communications Hubs, at least 100,000 Communications Hubs are affected).

(d) The definition of "Responsible Supplier" shall be replaced with the following:

Responsible Supplier	means in respect of a Smart Metering System (or any Device forming, or intended to form, part of a Smart Metering System) or a SMETS1 Installation (or any Device forming part of a SMETS1 Installation) which relates to: (a) an MPAN, the Import Supplier for the Electricity Meter that forms part of that Smart Metering System or SMETS1 Installation; and/or (b) an MPRN, the Gas Supplier for the Gas Meter that forms part of that Smart Metering System or SMETS1 Installation.

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

Commissioning Party	Shall mean the DCC when performing the tasks ascribed to the Commissioning Party in this Code.
Commissioning Party Systems	That part of the DCC Total System used for the purposes referred to in sub-paragraph (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.

(f) an additional rule of interpretation shall apply such that words beginning with capital letters which are defined in this TMAD and used elsewhere in this Code shall, unless the context otherwise requires, have the meanings given to them in this TMAD; and

(g) the definitions set out below shall be added to Section A or, where they already exist in Section A, they shall be replaced with the meanings set out below:

Application Association	has the meaning given to that expression in the DLMS COSEM Green Book (DLMS UA 1000-2 Ed. 8), published by the DLMS User Association.
Authentication Key	has the meaning given to that expression in the DLMS COSEM Green Book (DLMS UA 1000-2 Ed. 8), published by the DLMS User Association.
Cryptographic Processing	means the generation, storage (other than of Secret Key Material used in relation to communications with a SMETS1 Device, where that Secret Key Material is encrypted) or use of any Secret Key Material.
Instruction	means, in respect of a SMETS1 Device, a communication generated by the SMETS1 Service Provider or a DCO following receipt of a SMETS1 Service Request by the DCC that is designed to instruct the Device to execute the functionality necessary to permit the DCC to take the necessary Equivalent Steps.
SMETS1 Symmetric Key	means an Authentication Key or a symmetric key which is in either case used to process communications with SMETS1 Devices.
Transport Layer Security	means TLS 1.2 as defined in the Internet Engineering Task Force (IETF) Request For Change (RFC) 5246 or any equivalent to that document which updates or replaces it from time to time.

3.1A No SMETS1 SMSO Systems (other than to the extent they are used to carry out Requesting Party activities) shall be considered to form part of the DCC Total System for the purposes of this Code.

Application of Appendix AC (Inventory Enrolment and Decommissioning Procedures)

3.2 The provisions of Clauses 3.4 and 3.5 of the Inventory Enrolment and Decommissioning Procedures shall not apply to the addition of SMETS1 Devices to the Smart Metering Inventory where those Devices form part of a SMETS1 Installation that is to be Migrated.

3.3 For the purposes of Migration, SMETS1 Devices may be added to the Smart Metering Inventory by the following organisations:

(a) in the case of a SMETS1 CHF, an S1SP; or

(b) in the case of any other SMETS1 Device, the Responsible Supplier for the Device or the Commissioning Party but, in either case, only in circumstances where the Device forms part of a SMETS1 Installation that is identified within a SMETS1 Commissioning File as having completed all the checks and processing referred to in Clause 5.27 without any failures flagged as 'Critical'.

Application of Appendix AG (Incident Management Policy)

3.4 Whilst this TMAD remains in force, Appendix AG shall be modified as follows:

(a) The definition of Live Services shall be replaced with the following definition:

Live Services	Means: (a) any of the Services that the DCC is obliged to provide to a User, an Authorised Subscriber, a DCC Gateway Party (once its connection is capable of operation), but excluding Testing Services; (b) the exchange of data pursuant to Section E2; and (c) any of the Services provided pursuant to the TMAD.

3.5 The provisions of the Incident Management Policy shall apply to Migration Incidents provided that the following variations shall apply:

(a) Clause 2.1.3 of Appendix AG shall not apply in respect to Migration Incidents;

(b) Clause 5.2 of Appendix AG shall not apply in respect of DCC Migration Systems;

(c) where the DCC ought to be reasonably able to resolve a Migration Incident without the assistance of any Responsible Supplier, or the DCC ought to be able to arrange for the relevant SMETS1 SMSO to do so without the assistance of any Responsible Supplier, any incident resolution activities associated with a Migration Incident shall be assigned to the DCC; otherwise the incident resolution activities shall be assigned to the Responsible Supplier;

(d) except where an Incident is required to be raised by the DCC pursuant to this TMAD, the DCC shall not be required to raise an Incident, and no Party shall have the right to raise an Incident, in circumstances where a Responsible Supplier or the SMETS1 SMSO is notified by the DCC

in accordance with this TMAD that one or more of the steps in the Migration of a SMETS1 Installation have not been successfully completed; and

(e) Table 1 in Clause 2.4 of Appendix AG shall be replaced with the following Table:

Incident Category	**Description**	**Target Initial Response Time**	**Target Resolution Time**
1	A Category 1 Incident (Major Incident) is an Incident which, in the reasonable opinion of the DCC: • prevents a large group of Incident Parties from using the Live Services; • has a critical adverse impact on the activities of the Incident Parties using the Live Services of the DCC; • has a critical adverse impact on the activities necessary to Migrate SMETS1 Installations comprising Dormant Meters pursuant to the Transition and Migration Approach Document; • causes significant financial loss and/or disruption to the Incident Parties; or • results in any material loss or corruption of DCC Data. For a Major Security Incident there are additional considerations: • HMG, through CPNI, have declared a Major Incident based on their procedures; • a pattern has been seen across the DCC Total System that in total would have a significant security impact; or • Data covered by the Data Protection Act has either been lost or obtained by an unauthorised party, or is seriously threatened.	10 minutes	4 hours

2	An Incident which in the reasonable opinion of the DCC: • has a non-critical adverse impact on the activities of Incident Parties, but the Live Service is still working at a reduced capacity; • causes financial loss and/or disruption to other Incident Parties which is more than trivial but less severe than the significant financial loss described in the definition of a Category 1 Incident; or • has a non-critical adverse impact on the activities necessary to Migrate SMETS1 Installations comprising Dormant Meters pursuant to the Transition and Migration Approach Document.	20 minutes	24 hours
3	An Incident which, in the reasonable opinion of the DCC: • has an adverse impact on the activities of an Incident Party but which can be reduced to a moderate adverse impact due to the availability of a workaround; • has a moderate adverse impact on the activities of an Incident Party; or • has a moderate adverse impact on the activities necessary to Migrate SMETS1 Installations comprising Dormant Meters pursuant to the Transition and Migration Approach Document.	45 minutes	72 hours
4	An Incident which, in the reasonable opinion of the DCC: • has a minor adverse impact on the activities of an Incident Party; or • has a minor adverse impact on the activities necessary to Migrate SMETS1 Installations comprising Dormant Meters pursuant to the Transition and Migration Approach Document.	3 hours	5 days

5	An Incident which, in the reasonable opinion of the DCC: • has minimal impact on the activities of Incident Party; or • has minimal impact on the activities necessary to Migrate SMETS1 Installations comprising Dormant Meters pursuant to the Transition and Migration	1 day	10 days

Application of Section F (Smart Metering System Requirements)

3.6 Whilst this TMAD remains in force, for the purposes of Section F2.10A (SMETS1 Lists), each entry on each of the SMETS1 Pending Product Combinations and SMETS1 Eligible Products Combinations lists shall, in addition to setting out a combination of Device Models and communication services provider, additionally identify, in relation to that entry, the SMETS1 SMSO, and whether that entry applies to SMETS1 Installations comprising either (i) solely Dormant Meters (ii) solely Active Meters; or (iii) either Dormant Meters and/or Active Meters. Where either list contains two or more entries that have the same combination of Device Models but identify different SMETS1 SMSOs and/or different permitted combinations of Active Meters / Dormant Meters, each entry shall be treated as a separate entry for the purpose of the list and the requirements of Section H5.8 shall be modified accordingly so that the words "listed on the SMETS1 Eligible Product Combinations" (in both places that they appear) are replaced with "which match all of the characteristics of an entry on the SMETS1 Eligible Product Combinations". The requirements of Section H5.9 shall be modified so that the words "that is listed on the SMETS1 Eligible Products Combinations" are replaced with "which match all of the characteristics of an entry on the SMETS1 Eligible Product Combinations".

3.7 With the exception of those that arise as a consequence of SMETS1 Pending Product Combination Tests, the DCC shall not add an entry to the list of SMETS1 Eligible Product Combinations other than to the extent that it has the approval of the Secretary of State to do so. In the case of a manifest error in the submission, approval and/or addition of an entry to the list of SMETS1 Eligible Product Combinations the Secretary of State may take such steps as are reasonably necessary to correct for such error(s) and/or direct the DCC to take such steps as are reasonably necessary to correct the error(s). The DCC shall promptly notify all SEC Parties, the Panel, the Authority and the Secretary of State where steps are taken to correct errors pursuant to this Clause 3.7.

Application of Section G (Security)

3.8 For the purposes of Section G (with the exception of Sections G2.19 to G2.24 inclusive), no Requesting Party Systems shall be considered to form part of the DCC Total System; provided that the DCC shall ensure that the requirements of Clause 11 are met in relation to each Requesting Party and each associated SMETS1 SMSO.

3.9 The Commissioning Party Systems shall not be considered to form part of the DCC Live Systems for the purposes of Sections G2.23, G2.25, G3.13 or G3.14.

3.10 Whilst this TMAD remains in force, the following additional requirement shall apply under Section G4 (Organisational Security: Obligations on Users and the DCC): The DCC shall ensure that no individual is engaged in:

(a) the development of bespoke software or firmware, or the customisation of any software or firmware, for the purpose of its installation on any part of the Commissioning Party Systems; or

(b) the development, design, build, testing, configuration, implementation, operation, maintenance, modification or decommissioning of any part of the Commissioning Party Systems,

unless that individual satisfies the requirements of Clause 3.11.

3.11 An individual satisfies the requirements of this Clause only if, at any time at which that individual is engaged in any activity described in Clause 3.10, he or she:

(a) is not at the same time also engaged in:

(i) the development of bespoke software or firmware, or the customisation of any software or firmware, for the purpose of its installation on any Smart Metering Inventory Systems; or

(ii) the development, design, build, testing, configuration, implementation, operation, maintenance, modification or decommissioning of any Smart Metering Inventory Systems; and

(b) has not been engaged in any activity described in paragraph (a) for a period of time which the DCC reasonably considers to be appropriate, having regard to the need to ensure the management of risk in accordance with the DCC Information Security Management System.

3.12 Whilst this TMAD remains in force, the following additional requirement shall apply under

Section G2 (System Security: Obligations on the DCC):

(a) The DCC shall ensure that no resources which form part of the Commissioning Party Systems also form part of its Smart Metering Inventory Systems.

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

3.14 The DCC shall ensure that Anomaly Detection Thresholds set in relation to the Commissioning Party are 0 for all requests that are not Commissioning Requests.

3.14A Whilst this TMAD remains in force, Sections G2.44, (where it exists) G2.44A, and G2.45 shall be replaced by the following:

G2.44 The DCC shall ensure that all Cryptographic Processing which:

(a) is for the purposes of complying with its obligations as CoS Party;

(b) results in the application of a Message Authentication Code to any message in order to create a Command to be sent to a SMETS2+ Device;

(c) is carried out by a DCO and involves the use of a SMETS1 Symmetric Key;

(d) involves the use of a DCC Private Key to establish any Transport Layer Security for the purposes of communicating with a SMETS1 Device; or

(e) (other than in any of the circumstances set out in Section G2.44A) is carried out by a SMETS1 Service Provider and involves the use of a SMETS1 Symmetric Key,

is carried out within Cryptographic Modules which are compliant with FIPS 140-2 Level 3 (or any equivalent to that Federal Information Processing Standard which updates or replaces it from time to time).

G2.44A For the purposes of Section G2.44(e), the circumstances set out in this Section G2.44A shall be those in which one of the following occurs:

(a) Cryptographic Processing is carried out by a SMETS1 Service Provider to generate a Command to "add credit" (as specified in a Version of the SMETS with a Principal Version number of 1) to a SMETS1 Device;

(b) a SMETS1 Symmetric Key is used by a SMETS1 Service Provider to generate an Instruction where the target Device is identified in the SMETS1 Supporting Requirements as a Category 1 Device for the purposes of this paragraph (b);

(c) a SMETS1 Symmetric Key is used by a SMETS1 Service Provider where:

(i) that Symmetric Key is valid only for the duration of a single Application Association; and

(ii) the target Device is identified as a Category 2 Device for the purposes of this sub-paragraph in the SMETS1 Supporting Requirements; or

(d) there is any use of a SMETS1 Symmetric Key where:

(i) the initial value of that key value is provided to the DCC by a Requesting Party in a Migration Group Encrypted File; and

(ii) the DCC is required to stop using that initial key value either:

(A) during Migration of the SMETS1 Installation, as required by this TMAD; or

(B) within 7 days of that Migration, as required by Clause 20.1 of the SMETS1 Supporting Requirements.

G2.45 The DCC shall ensure that any and all Cryptographic Processing undertaken under or pursuant to this Code which does not fall within the scope of Section G2.44 is carried out within Cryptographic Modules established in accordance with its Information Classification Scheme.

3.14B For GroupID = “DA”, the DCC shall, in relation to each Relevant Device during the UTRN Period for that Device, ensure that any request to generate a SMETS1 UTRN for a non-negative prepayment top-up in relation to that Device that;

(a) is received by the SMETS1 SMSO; and

(b) had it been received prior to the commencement of the UTRN Period, would have been processed by the SMETS1 SMSO,

is processed by the SMETS1 SMSO and/or the SMETS1 Service Provider (as the case may be) in materially the same manner (including to have the same effect on the Relevant Device)

as it would have had, if it had been processed by the SMETS1 SMSO prior to the commencement of the UTRN Period.

3.14C The DCC shall ensure that the SMETS1 SMSO for GroupID = "DA":

(a) is not capable of generating a SMETS1 UTRN in relation to a SMETS1 Device after the S1SP has successfully processed a Service Request with Service Reference Variant 8.1.1 for that SMETS1 Device as set out in Clause 8.1 and Table 8.7.2; and

(b) does not provide any response to a request to generate a SMETS1 UTRN in relation to such a SMETS1 Device after the step in Clause 3.14C(a), other than a response that is generated by the relevant S1SP in accordance with Clause 3.14D below.

3.14D For GroupID = "DA":

(a) during the UTRN Period for an ESME or GSME and where the S1SP receives a request to generate a SMETS1 UTRN for such a SMETS1 Device from the SMETS1 SMSO, the S1SP shall send a UTRN for the Relevant Device, that is consistent with the request, to that Device and/or to that SMETS1 SMSO; and

(b) after the UTRN Period ends for the Relevant Device, shall only send a response to the SMETS1 SMSO that indicates that the request to generate a UTRN has been unsuccessful.

3.14E The DCC shall ensure that, by no later than 15 months after the Last EPCL Entry for the S1SP related to the GroupID = "DA", all interfaces to the Systems of that S1SP that are not required by the DCC for the provision of Services under this Code (excluding any amendments to those Services made by virtue of this TMAD) are securely and irrevocably disconnected from the Systems of the S1SP.

3.14F The DCC shall as soon as reasonably practicable following the carrying out of the steps referred to in Clause 3.14E, obtain an independent audit and provide to the SMKI PMA and the Security Sub-Committee the report of that audit confirming that the steps have been properly and successfully carried out together with any remediation plan that may be required.

Application of Section H (DCC Services)

3.15 Whilst this TMAD remains in force:

(a) As soon as reasonably practical after this TMAD comes into effect, each User shall provide the DCC with an additional forecast under Section H3.22 (Managing Demand for DCC User Interface Services) of the number of Service Requests in respect of SMETS1 Devices that the User will send in each of the 8 months following the end of the month in which such forecast is provided;

(b) Section H8.3(a) (Maintenance of the DCC Systems) shall not apply in respect of the DCC Migration Systems. The DCC may undertake Planned Maintenance of the DCC Migration Systems at any time during any day, provided that the DCC shall only undertake such maintenance when it is not likely to have an adverse impact on the ability to Migrate the number of SMETS1 Installations that the DCC has committed to Migrate on that day;

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

(g) Section H5.8 of the Code shall be modified in accordance with the provisions of Clause 3.6 of TMAD.

Application of Section L (Smart Metering Key Infrastructure and DCC Key Infrastructure)

3.16 Whilst this TMAD remains in force, the table in Section L3.18 (Organisation Certificates) shall be replaced with the following 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)
issuingAuthority	The DCC	[Not applicable]	(a)
networkOperator	A Network Party	Either: (a) Electricity Distributor; or (b) Gas Transporter.	[Not applicable]
supplier	A Supplier Party	Either: (a) Import Supplier; or (b) Gas Supplier.	[Not applicable]
Other	An RDP or any Party other than the DCC	Either: (a) Other User; (b) Registered Supplier Agent; (c) Registration Data Provider; or (d) Export Supplier.	[Not applicable]
pPPXmlSign	The DCC	[Not Applicable]	(g)
pPRDPFileSign	The DCC	[Not Applicable]	(g)

s1SPxmlSigning	The DCC	[Not Applicable]	(g)
commissioningPartyFileSigning	The DCC	[Not Applicable]	(j)
requestingPartyFileSigning	The DCC	[Not Applicable]	(i)
s1SPMigrationSigning	The DCC	[Not Applicable]	(h)
commissioningPartyXmlSigning	The DCC	[Not Applicable]	(j)

Application of Section M (General)

3.17 The Responsible Supplier for each Device referred to in Clause 4.26 of this TMAD acknowledges that the carrying out of one or more of the steps referred to in this TMAD, at the request of the DCC, may result in the loss of Data stored on or in relation to each such Device and/or the ability to utilise the functionality of the Device. Neither the DCC nor the Installing Supplier shall be liable to the Responsible Supplier (or any other Party) for any Liability that arises from the carrying out of (or attempt to carry out) any of those steps, at the request of the DCC, where (and to the extent that) such person has acted in accordance with Good Industry Practice.

3.18 Where a Supplier Party has agreed with a SMETS1 SMSO that the SMETS1 SMSO shall not permit any third parties to communicate or otherwise interfere with a SMETS1 Installation (or any Devices forming part of it), then that Supplier Party confirms that that SMETS1 SMSO may permit the DCC to take the steps provided for in this TMAD which results in a communication or interference with that SMETS1 Installation (or any Devices forming part of it). Notwithstanding Section M11.6 of the Code, the SMETS1 SMSO shall be entitled to rely on and enforce the confirmation in this Clause 3.18 under the Contract (Rights of Third Parties) Act 1999.

3.19 It is acknowledged that each SMETS1 SMSO is acting as a DCC Service Provider when performing tasks ascribed to a SMETS1 SMSO under this TMAD (including where the SMETS1 SMSO provides services to the DCC in order for the DCC to carry out the tasks ascribed to a Requesting Party), and notwithstanding Section M11.6 of the Code, is therefore a person under Section M11.5 of the Code and entitled to rely on the waiver in Section M2.13(a) of the Code.

3.20 The DCC shall provide the Services described in this TMAD in accordance with Good Industry Practice. Each Installing Supplier shall act in accordance with Good Industry Practice when

providing the support or assistance referred to in Clause 4.33.

3.21 The DCC shall take reasonable steps to ensure that any Data that is provided to it by each SMETS1 SMSO, for the purposes of Migration, is accurate.

3.22 Each Party's liability under and in connection with this TMAD is limited in accordance with Section M2 (Limitations of Liability), provided that the liability of each of the DCC and each Installing Supplier for failing to act in accordance with Good Industry Practice in relation to the carrying out of (or attempt to carry out) one or more of the steps referred to in Clause 4.26 of this TMAD (and/or, in the case of the Installing Supplier, the provision of support or assistance referred to in Clause 4.33) shall be limited to £1,000,000 in the aggregate for each period of 12 months from the date this TMAD comes into effect (and from each anniversary of such date); and further provided that the DCC and/or relevant Installing Supplier will not be liable for a claim unless the claiming Party has given notice of such claim within six months of the occurrence of the relevant failure.

3.23 Where necessary, the provisions of Section M2.5(d) shall apply in relation to any liability that has been limited by the provisions of Clause 3.22.

4 Pre-Migration Rights and Obligations

4.1 Each Supplier Party shall provide any information that the DCC reasonably requests in order to support the planning, coordination and undertaking of (and ongoing support for) the Migration of SMETS1 Installations, and shall do so in the timescales that the DCC reasonably requests.

4.2 Where and to the extent notified by the DCC, each Supplier Party may request that the DCC undertakes early validation of any Migration Common Files pertaining to SMETS1 Installations comprising an Active Meter for which it is the Responsible Supplier. To enable this, the DCC shall permit each SMETS1 SMSO to make arrangements with the relevant Requesting Party to enable the submission of Migration Common Files for early validation purposes, provided that such files shall be submitted to a different location from those submitted by the Requesting Party pursuant to Clause 5.8. When the DCC receives such a file, it shall carry out the steps required by Clauses 5.9 and 5.10.

4.3 Subject to Clause 4.24, the DCC shall, on any day during which it is carrying out the Migration of SMETS1 Installations, take reasonable steps to Migrate relevant SMETS1 Installations flagged as a priority prior to SMETS1 Installations not flagged as a priority.

4.4 Where, by virtue of this TMAD, the DCC is required to consult on the content of any document with the Panel, all Parties, the Authority and (on request) the Secretary of State prior to such a document taking effect, this requirement may be satisfied by the undertaking of consultation on such content prior to this TMAD coming into effect.

Indicative Migration Forecasts and Migration Demand Commitment

4.5 For the purposes of supporting the planning and coordination of the Migration of SMETS1 Installations, by no later than the 20th day of each month, each Responsible Supplier shall provide an Indicative Migration Forecast to the DCC for each SMETS1 SMSO. Such forecast shall, at a minimum, be broken down by Electricity Distributor and shall be provided in relation to any SMETS1 SMSOs in relation to which Migration is due to commence within the next six months (as set out in the SMETS1 Services delivery plan produced pursuant to condition 13 of the DCC Licence).

4.6 By the end of each month, the DCC shall provide all Parties, the Panel, the Authority and the Secretary of State with a summary report that aggregates information from all Indicative Migration Forecasts showing the aggregate forecast number of SMETS1 Installation Migrations per day and per SMETS1 SMSO.

4.7 The DCC may provide to a SMETS1 SMSO all Indicative Migration Forecasts provided to it by Responsible Suppliers that pertain to that SMETS1 SMSO.

4.8 The DCC and each Responsible Supplier shall schedule the Migration of SMETS1 Installations comprising an Active Meter(s) that pertain to a particular SMETS1 SMSO in each Migration Week in accordance with the following process:

(a) by no later than 10.00 hours on the Tuesday that falls three weeks and six days prior to each Migration Week, each Responsible Supplier shall notify the DCC, of the number of SMETS1 Installations in relation to which it reasonably expects to submit Migration Authorisations for each day of that Migration Week, per day and identify the number of those SMETS1 Installations per day per SMETS1 SMSO (the "Daily Migration Demand") and this Daily Migration Demand will be dis-aggregated by Electricity Distributor;

(b) by no later than 10.00 hours on the following Tuesday, the DCC shall confirm to each Responsible Supplier the number of SMETS1 Installations that the DCC is committing to Migrate on each day within that Migration Week for that Responsible Supplier per SMETS1 SMSO (the "Migration Demand Commitment"), which shall, subject to Clause 4.11, be the

same as the Responsible Supplier's Daily Migration Demand; and

(c) by no later than 17.00 hours on that same following Tuesday, the DCC shall provide all Parties, the Panel, the Authority and the Secretary of State with a summary report that aggregates information from all Migration Demand Commitments, which includes the number of SMETS1 Installations dis-aggregated by Electricity Distributor in that Migration Week per SMETS1 SMSO, or where necessary a pro-rata estimate of this.

4.9 Where a Responsible Supplier does not notify the DCC of the Responsible Supplier's Daily Migration Demand for any particular Migration Week in accordance with Clause 4.8(a), the DCC shall use the most recently, previously notified Daily Migration Demand for that Responsible Supplier for the purposes of its migration scheduling in relation to that Migration Week.

4.10 Where pursuant to Clause 4.8(b), the DCC fails to confirm the Migration Demand Commitment for a Responsible Supplier, the DCC shall be deemed to have agreed to and confirmed that the Responsible Supplier's Daily Migration Demand for each day per SMETS1 SMSO within the relevant Migration Week is that Supplier's Daily Migration Demand Commitment.

4.11 Where the DCC reasonably considers that it cannot commit to the value for a Daily Migration Demand for one or more days within any future Migration Week, the DCC shall set each Responsible Supplier's Daily Migration Demand Commitment in accordance with the rules set out in a document for that purpose (the "**Migration Scaling Methodology**"), as described in Clause 4.12.

4.12 The DCC shall make available to the Panel, all Parties, the Authority and (on request) the Secretary of State the Migration Scaling Methodology, as follows:

(a) the DCC shall establish and periodically review the Migration Scaling Methodology, and shall consult with the Panel, the Parties and the Authority on the content of or any subsequent modification to the Migration Scaling Methodology prior to it taking effect; and

(b) at least 14 days prior to the coming into effect of the Migration Scaling Methodology or any subsequent revision to it, the DCC shall provide a copy of that document to the Panel, the Parties, the Authority and the Secretary of State, and publish a copy of it on the DCC Website.

4.13 Where a Party disagrees with the content of any version of the Migration Scaling Methodology, the Party may (within one month of that version coming into effect) refer the matter to the Secretary of State for their determination, which determination shall be final and binding for

the purposes of the Code. In the event that such referral is made the new version of the Migration Scaling Methodology published by the DCC shall apply prior to any such determination.

4.14 The DCC shall, in relation to each Responsible Supplier, take all reasonable steps to Migrate each day a number of SMETS1 Installations that contain one or more Active Meters for which that Supplier Party is the Responsible Supplier that is equal to the number within the Migration Demand Commitment for that Responsible Supplier, subject to having received the necessary Migration Authorisation to do so. For each Migration Week, the DCC shall, as soon as reasonably practicable, notify the relevant Responsible Supplier where the DCC reasonably considers that it will only be able to Migrate a number of SMETS1 Installations for that Responsible Supplier that is materially less than the number within the Migration Demand Commitment for that Responsible Supplier.

4.15 For each Responsible Supplier, the DCC may Migrate further SMETS1 Installations each day in excess of the Migration Demand Commitment for that Responsible Supplier where the DCC considers it is reasonable to undertake such additional Migrations and where a Migration Authorisation has been submitted for the excess.

Pre-conditions for Migration

4.16 The Requesting Party shall not commence the Migration of any SMETS1 Installation that does not correspond to an entry on the SMETS1 Eligible Product Combinations.

4.17 The Requesting Party shall not commence the Migration of any SMETS1 Installation until the DCC has received (or is deemed to have received in accordance with Clause 4.26(a) or the definition of Migration Authorisation) a Migration Authorisation from the Responsible Supplier or Responsible Suppliers for that SMETS1 Installation.

4.18 Each Supplier Party agrees that where the DCC has received (or is deemed to have received in accordance with Clause 4.26(a) or the definition of Migration Authorisation) such Migration Authorisation(s), it may carry out the steps to Migrate that SMETS1 Installation in accordance with the provisions of this TMAD.

4.19 Where there is more than one Responsible Supplier for a SMETS1 Installation and where the DCC has received Migration Authorisations from both such Responsible Suppliers which authorise the Migration of that SMETS1 Installation on different days in the same Migration Week, the Requesting Party shall take steps to initiate the Migration of that SMETS1

Installation in timescales consistent with the later of those two days. In such circumstances, the Migration Authorisation provided by the Responsible Supplier for the earlier of the two days is deemed amended to constitute a Migration Authorisation for the later of those two days.

4.20 Each Supplier Party agrees that each SMETS1 SMSO and the DCC may exchange any information (including Secret Key Material) that is reasonably needed for the DCC to discharge any of its obligations under this TMAD.

4.21 The DCC shall, from time to time, use and rely upon (and shall, subject to Clause 3.21, have no liability arising from any inaccuracy in) the information provided to it by each SMETS1 SMSO for the purposes of this TMAD, including:

(a) the Device IDs of Devices that are to be Migrated;

(b) the status of Devices, being 'Dormant Meter', 'Active Meter' or 'Active GPF';

(c) MPANs and MPRNs associated with Devices; and

(d) the content of Migration Common Files, Migration Group Files and Migration Group Encrypted Files.

4.22 This TMAD constitutes each Responsible Supplier's documented instructions to the DCC and each SMETS1 SMSO to Process any Personal Data required for the purposes of Migration of SMETS1 Installations.

4.23 With the exception of GroupID = DA, the DCC shall, where requested to do so by a Responsible Supplier for one or more SMETS1 Installations comprising an Active Meter for which that Supplier is the Responsible Supplier, take all reasonable steps not to start the Migration of those SMETS1 Installations notwithstanding that the DCC has previously received a Migration Authorisation in respect of them from the Responsible Supplier.

4.23A For GroupID = DA where requested by a Responsible Supplier, the DCC shall take all reasonable steps not to start the Migration of any SMETS1 Installation for which that Supplier Party is a Responsible Supplier for one (or both) Active Meters. The effect of this shall be that where DCC can accommodate the request, the DCC shall not start the Migration of any of the SMETS1 Installations contained in any Migration Authorisation received from that Responsible Supplier that are due to commence on the same day as the SMETS1 Installation(s) that was the subject of the request, for which the Migration has not yet commenced.

Dormant Meters

4.24 The DCC shall take all reasonable steps to Migrate SMETS1 Installations comprising only Dormant Meters, including arranging for any pre-requisite steps set out in this TMAD to be undertaken. The DCC shall Migrate SMETS1 Installations comprising only Dormant Meters as soon as reasonably practicable, which shall include giving priority to the Migration of SMETS1 Installations comprising only Dormant Meters over and above SMETS1 Installations which include one or more Active Meters.

4.25 Each Responsible Supplier for each SMETS1 CHF that forms part of a SMETS1 Installation that includes one or more Dormant Meters agrees that the relevant SMETS1 SMSO may, where requested to do so by the DCC, initiate remote communications with that SMETS1 CHF in order to confirm whether or not the SMETS1 SMSO is capable of remotely communicating with that SMETS1 CHF.

4.26 The Responsible Supplier for each Dormant Meter and any associated Devices for which it is also the Responsible Supplier that form part of a SMETS1 Installation agrees that the relevant SMETS1 SMSO may, where requested to do so by the DCC, take any steps reasonably necessary in order to ensure that the Devices are configured in accordance with the requirements of the SMETS1 Supporting Requirements and Clause 5.12(e) of this TMAD, and/or such that the Devices form part of a SMETS1 Installation that comprises an entry on the list of Eligible Product Combinations, including upgrading the firmware on the Devices for those purposes. The Responsible Supplier for each Dormant Meter and any associated Devices for which it is also the Responsible Supplier that form part of a SMETS1 Installation agrees that the relevant SMETS1 SMSO may, where requested to do so by the DCC, take any steps reasonably necessary in order to upgrade the firmware on the Devices such that the Devices form part of an entry that is planned to be listed on the Eligible Product Combinations. For the purposes of this Clause 4.26, an entry is planned to be listed on the Eligible Product Combinations where pursuant to the SEC Variation Testing Approach Document for SMETS1 Services:

(a) a Completion Report for the Migration Test Phase and SIT Test Phase regarding the planned entry on the list of Eligible Product Combinations has been approved by the TAG; or

(b) a DMCT EPCL Report has been issued in respect of the planned entry on the list of Eligible Product Combinations.

4.27 The Responsible Supplier for each Device referred to in Clause 4.26, authorises the DCC to

take the steps and carry out the processing set out in this TMAD in order to Migrate the relevant SMETS1 Installation (and is therefore deemed to have given a Migration Authorisation in respect of that SMETS1 Installation).

4.28 Where a SMETS1 Installation includes both an Active Meter and a Dormant Meter, the DCC shall not commence the Migration unless it has received a Migration Authorisation from the Responsible Supplier for the Active Meter in relation to that SMETS1 Installation.

4.29 Where the DCC plans to carry out the steps referred to in Clause 4.26 in relation to any SMETS1 Installation which includes Dormant Meters (but no Active Meters), the DCC shall notify the Responsible Supplier(s) for that SMETS1 Installation at least 5 Working Days (or fewer where mutually agreed between the DCC and the Responsible Supplier(s) for that SMETS1 Installation) before the earliest scheduled date for undertaking those steps. Where there are two Responsible Suppliers for the Smart Metering Systems that together comprise the same SMETS1 Installation that contains only Dormant Meters, and they are Affiliates of one another, then the DCC may issue such notification only to the Responsible Supplier for the Electricity Smart Metering System and the Responsible Supplier for the Gas Smart Metering System shall be deemed to have received a notification for the purpose of this Clause 4.29. Where there is a change of Responsible Supplier after the DCC has issued such notification, the DCC may continue to carry out the relevant steps as planned and shall take reasonable steps to notify the new Responsible Supplier prior to carrying them out.

4.30 Where the DCC plans to carry out the steps referred to in Clause (a) in relation to any SMETS1 Installation which includes Dormant Meters (but no Active Meters), the DCC shall notify the Responsible Supplier(s) for that SMETS1 Installation at least 15 Working Days (or fewer where mutually agreed between the DCC and the Responsible Supplier(s) for that SMETS1 Installation) before the earliest scheduled date for undertaking those steps. Where there are two Responsible Suppliers for the Smart Metering Systems that together comprise the same SMETS1 Installation that contains only Dormant Meters, and they are Affiliates of one another, then the DCC may issue such notification only to the Responsible Supplier for the Electricity Smart Metering System and the Responsible Supplier for the Gas Smart Metering System shall be deemed to have received a notification for the purpose of this Clause 4.30. Where there is a change of Responsible Supplier after the DCC has issued such a notification, the DCC may continue carry out the relevant steps as planned and shall take reasonable steps to notify the new Responsible Supplier prior to carrying them out.

4.31 Notifications sent by the DCC pursuant to Clause 4.29 or Clause 4.30 shall be processed in

accordance with the Migration Authorisation Mechanism and shall include, as a minimum, in relation to each SMETS1 Installation:

(a) the date from which the DCC has scheduled the relevant activities;

(b) the relevant MPANs and MPRNs;

(c) the Device ID for each relevant Device;

(d) the device serial number (according to information held by the relevant SMETS1 SMSO) for each relevant Device; and

(e) where such notification is sent pursuant to Clause 4.29, the Device Model Combination that the DCC intends should result from any firmware upgrades that it plans to instruct in relation to the relevant Device(s).

4.32 Where a Responsible Supplier receives a notification from DCC pursuant to Clause 4.30 the Responsible Supplier may respond in the manner set out in the Migration Authorisation Mechanism to flag any notified SMETS1 Installation as a priority and/ or to specify the Supplier and/or Network Operator Certificate IDs that it wishes the DCC to include in Commissioning Requests that it processes in relation to any notified SMETS1 Installation. Where there are two Responsible Suppliers for the Smart Metering Systems that together comprise the same SMETS1 Installation, and they are Affiliates of one another, then the Responsible Supplier for the Electricity Smart Metering System may specify the Supplier and/or Network Operator Certificate IDs that it wishes the DCC to include in Commissioning Requests in respect of the Gas Smart Metering System, in which case the Responsible Supplier for the Gas Smart Metering System shall be deemed to have specified those Supplier and/or Network Operator Certificate IDs. The DCC shall only be obliged to consider such information where it is received within the timescales set out in the Migration Authorisation Mechanism but may use such information submitted after these timescales if it is practicable to do so. A Supplier Party may only request that a SMETS1 Installation is treated as a priority for Migration purposes where the type of Energy Consumer at the premises for that SMETS1 Installation requires it to be prioritised over and above the Migration of other SMETS1 Installations.

4.33 Any Supplier Party that is an Installing Supplier for any of the Dormant Meters and associated Devices referred to in Clause 4.26 shall take all reasonable steps to provide such support and assistance as the DCC may reasonably request (including where they exist, the provision of firmware for each such Device) in order that the DCC or the relevant SMETS1 SMSO is

capable of carrying out the steps set out in Clause 4.26. For the purposes of carrying out the steps that are set out in Clause 4.26, the DCC and/or any relevant SMETS1 SMSO shall rely on (and shall have no liability arising from any inaccuracy in) the firmware that is provided to the DCC by an Installing Supplier together with the relevant information that supports the sequencing of the required firmware upgrades, unless it is (or should reasonably have been) apparent to the DCC that the firmware or relevant information that has been provided to the DCC is not suitable.

4.34 The DCC shall provide to any Supplier Party upon request relevant excerpts from the information provided to it pursuant to Clause 4.33 in relation to sequencing of firmware upgrades and/or configuration of devices. No Party shall have any liability arising from any inaccuracy in the information provided by the DCC pursuant to this Clause 4.34.

4.34A Where there is more than one SMETS1 PPMID, SMETS1 IHD or SMETS1 CAD in a SMETS1 Installation, that is comprised solely of Dormant meters, the DCC shall include only one of each Device Type in the Migration Common File, which shall be the one that was most recently joined to the HAN. Any SMETS1 PPMID, SMETS1 IHD or SMETS1 CAD for which there is insufficient information in order to populate the Migration Common File shall not be included in the MCF and therefore shall not be Migrated.

Migration Authorisations and the Migration Authorisation Mechanisms

4.35 The DCC shall set out and make available to all Supplier Parties the proposed mechanism (the "Migration Authorisation Mechanism") which shall, in addition to the matters set out in Clauses 4.29 to 4.32, provide the means by which:

(a) a Migration Authorisation may be provided by the Responsible Supplier(s) for a SMETS1 Installation comprising one or more Active Meters to the Requesting Party;

(b) where the Responsible Supplier is the Responsible Supplier for all Devices comprising a SMETS1 Installation comprising only Active Meters, the Responsible Supplier shall indicate whether it wishes the Commissioning Party to carry out the steps necessary to Commission the Devices comprising that SMETS1 Installation or, alternatively that the Responsible Supplier wishes itself to carry out these steps, being, as further described in Clauses 4.37 to 4.40; and

(c) Clause 4.35 (b) shall also apply where there are two Responsible Suppliers for the Smart Metering Systems that together comprise the same SMETS1 Installation comprising only Active Meters, and they are Affiliates of one another, in which case the Responsible Supplier

for the Electricity Smart Metering System shall give the required indication on behalf of itself and the Responsible Supplier for the Gas Smart Metering System (and any such indication shall be deemed to constitute an indication by the Responsible Supplier for the Gas Smart Metering System) provided that the indication is either that both Responsible Suppliers wish the Commissioning Party to carry out the steps, or both Responsible Suppliers wish themselves to carry out the steps.

4.36 Where a SMETS1 Installation includes any Dormant Meter, the steps that are necessary to Commission the Devices that comprise that SMETS1 Installation shall only be carried out by the Commissioning Party.

4.37 Where a SMETS1 Installation includes both an Active Meter and a Dormant Meter, the DCC shall notify the Responsible Supplier, that is the Responsible Supplier for the Active Meter in relation to that SMETS1 Installation, by no later than 23:59 on the Thursday that falls three days prior to the Migration Week in which that SMETS1 Installation is scheduled for Migration, that the SMETS1 Installation includes a Dormant Meter. Where the DCC receives a Migration Authorisation after the timescales for receipt set out in the Migration Authorisation Mechanism the DCC may still process Migrations based on the Migration Authorisation but shall not be obliged to do so.

4.38 The Migration Authorisation Mechanism shall require that the Responsible Supplier(s) for a SMETS1 Installation for which a Migration Authorisation is being provided shall provide the MPRN for each SMETS1 GSMS and/or the MPAN for each SMETS1 ESMS that forms part of that SMETS1 Installation. The Migration Authorisation Mechanism shall require that, in relation to each SMETS1 Device that forms part of a SMETS1 Installation for which Migration Authorisation is being provided, the Responsible Supplier for each Device listed in Table 4.38 shall provide the information required in that table for that Device. Where there are two Responsible Suppliers for the Smart Metering Systems that together comprise the same SMETS1 Installation comprising only Active Meters, and they are Affiliates of one another, the Responsible Supplier for the Electricity Smart Metering System may provide the required information for the SMETS1 ESME on behalf of itself and the required information for the SMETS1 GPF and SMETS GSME on behalf of the Responsible Supplier for the Gas Smart Metering System and this shall be deemed to constitute provision by the Responsible Supplier for the Gas Smart Metering System.

Device	**Required information**

SMETS1 ESME	CriticalSupplierCertificateID NonCriticalSupplierCertificateID
SMETS1 GPF	CriticalSupplierCertificateID NonCriticalSupplierCertificateID
SMETS1 GSME	CriticalSupplierCertificateID NonCriticalSupplierCertificateID

Table 4.38

4.39 The Migration Authorisation Mechanism shall require the Responsible Supplier that submits the Migration Authorisation to Digitally Sign communications containing Migration Authorisations using a Private Key associated with an IKI Certificate that has been Issued to an Authorised Responsible Officer of that Responsible Supplier. More generally the DCC and Supplier Parties may use Private Keys associated with IKI Certificates that have been Issued to their Authorised Responsible Officers in order to Digitally Sign communications in relation to the Migration Authorisation Mechanism.

4.40 The Migration Authorisation Mechanism shall allow the Responsible Supplier to flag any SMETS1 Installation as a priority and/or to specify the Network Operator Certificate IDs that it wishes the DCC to include in Commissioning Requests that it processes. Where there are two Responsible Suppliers for the Smart Metering Systems that together comprise the same SMETS1 Installation, and they are Affiliated of one another, then the Responsible Supplier for the Electricity Smart Metering System may provide the Network Operator Certificate ID in respect of the Gas Smart Metering System, in which case the Responsible Supplier for the Gas Smart Metering System shall be deemed to have specified that Network Operator Certificate ID. A Supplier Party may only request that a SMETS1 Installation is treated as a priority for Migration purposes where the type of Energy Consumer at the premises for that SMETS1 Installation requires it to be treated as a priority.

4.41 The DCC shall, following consultation with Supplier Parties and after taking into account any comments that have been provided to it, publish the Migration Authorisation Mechanism to all Supplier Parties, together with the date on which it intends that the Migration Authorisation Mechanism shall come into effect, which shall be not less than 14 days from the date of

publication.

4.42 Following DCC's publication of the Migration Authorisation Mechanism and in accordance with the requirements of Clause 4.41 and prior to DCC's published date for the coming into effect of the Migration Authorisation Mechanism, any Supplier Party that wishes to object to the Migration Authorisation Mechanism may refer the matter to the Secretary of State for a determination, which determination shall be final and binding for the purposes of this TMAD.

4.43 The DCC may from time to time update the Migration Authorisation Mechanism, provided that the DCC shall ensure that the most up to date Migration Authorisation Mechanism is published to all Supplier Parties at all times. The processes set out in Clauses 4.41 and 4.42 shall apply to any modification of the Migration Authorisation Mechanism. The Migration Authorisation Mechanism published by the DCC shall have effect unless or until the Secretary of State determines otherwise.

4.44 The Responsible Supplier for each Active Meter and any associated Devices for which it is also the Responsible Supplier that form part of a SMETS1 Installation shall ensure that, prior to its Migration, the Devices that form part of that SMETS1 Installation are configured in accordance with the requirements of SMETS1 Supporting Requirements of this TMAD, and/or the Devices form part of a SMETS1 Installation that comprises a Device Model Combination that is listed on the Eligible Product Combinations, including upgrading the firmware on the Devices for those purposes.

4.44A Where there is more than one SMETS1 PPMID, SMETS1 IHD or SMETS1 CAD in a SMETS1 Installation, that is comprised of Active or Mixed Installations, the DCC shall include only one of each Device Type in the Migration Common File, which shall be the one that was most recently joined to the HAN. Any SMETS1 PPMID, SMETS1 IHD or SMETS1 CAD for which there is insufficient information in order to populate the Migration Common File shall not be included in the MCF and therefore shall not be Migrated.

Migration Reporting

4.45 The DCC shall make available to the Panel, all Parties and (on request) the Secretary of State the "Migration Reporting Regime" that list the reports that the DCC shall provide on Migration and provides an overview of the frequency, content of and recipients of those reports, as follows:

(a) the DCC shall establish and periodically review the Migration Reporting Regime, and shall

consult with the Panel, the Parties and the Authority on the content of or any subsequent modification to the Migration Reporting Regime prior to it taking effect; and

(b) at least 14 days prior to the coming into effect of the Migration Reporting Regime or any subsequent revision to it, the DCC shall provide a copy of that document to the Panel, the Parties, the Authority and the Secretary of State, and publish a copy of it on the DCC Website.

4.46 Where a Party considers that the reporting provided for in the Migration Reporting Regime made pursuant to Clause 4.45 is insufficient, the Party may (within one month of the document being provided under Clause 4.45) refer the matter to the Secretary of State for determination, which determination shall be final and binding for the purposes of this TMAD. In the event that such referral is made the new version of the Migration Reporting Methodology published by the DCC shall apply prior to any such determination.

Electricity Distributor Network Operator Certificate IDs

4.47 The DCC shall establish a reasonable process by which Electricity Distributors can notify the DCC of the Network Operator Certificate IDs that they wish the DCC to include in Commissioning Requests that the DCC processes in relation to SMETS1 ESMEs and shall inform Electricity Distributors of that notification process. The process shall allow an Electricity Distributor to change from time to time the Network Operator Certificate IDs that have been notified.

4.48 Where in relation to a SMETS1 ESME, the Responsible Supplier has not specified to the DCC either or both of the Electricity Distributor's Network Operator Certificate IDs in accordance with the Migration Authorisation Mechanism (for a SMETS1 ESME that is either an Active Meter or a Dormant Meter except where the SMETS1 ESME is a Dormant Meter and there is a SMETS1 GSME that is an Active Meter within the same SMETS1 Installation), the DCC shall (unless the DCC has identified that the relevant MPAN is invalid) ensure that, for any such unspecified Network Operator Certificate IDs, the latest Network Operator Certificate IDs that have been notified by the Electricity Distributor under Clause 4.47 are included in relation to the relevant Devices within any Migration Common File sent by the relevant Requesting Party.

5 Migration Process

Setup steps

5.1 Before the DCC adds an entry to the SMETS1 Eligible Product Combinations, the DCC shall,

for the Group which includes Devices with the corresponding combination of Device Models, notify to the relevant SMETS1 SMSO:

(a) where SMETS1 Installations for that Group, according to the Group Specific Requirements, require a Migration Group Encrypted File, the Public Keys that are to be used to create any required EncryptedS1SPGroupInformation or MasterKeyInformation elements and for each such Public Key:

(i) the Key Identifier (see X509SKI);

(ii) the inclusive start and end dates of the period during which the Public Key may be used; and

(iii) any constraints as to the part(s) of the Group in relation to which the Public Key can be used;

(b) and either

(i) the technical details and associated steps that would be required in order to configure Devices within such SMETS1 Installations and any associated systems, including those required by 'Pre-enrolment Configuration Requirements' for the specified GroupID, so as to be able to communicate with the DCC Live Systems; or

(ii) a statement that no such configuration would be required for Devices comprising such SMETS1 Installations.

5.2 When the DCC adds an entry to the SMETS1 Eligible Products Combinations, the DCC shall include within it the associated GroupID with that entry.

5.3 Any Private Key, which is associated with a Public Key published pursuant to Clause 5.1 for use in creating MasterKeyInformation elements, shall be generated by, and known only to, the relevant DCO.

5.4 Any Private Key, which is associated with a Public Key published pursuant to Clause 5.1 for use in creating EncryptedS1SPGroupInformation elements, shall be generated by, and known only to, the relevant S1SP.

5.4A Before the DCC adds the first entry to the SMETS1 Eligible Product Combinations with a GroupID = "DA", the DCO shall generate at least one Private Key and corresponding Public Key(s) for that GroupID to be used solely in relation to 'Securing a SMETS1 GSME' and

'Securing a SMETS1 ESME' for that GroupID in Appendix C. Such Private Key(s) shall be generated by, and known only to, the relevant DCO.

Digital Signature

5.5 In relation to the Digital Signing obligations in this TMAD, Parties shall only accept as valid Digital Signatures which authenticate against Certificates with Remote Party Roles conforming to Table 5.5. The Parties identified in Table 5.5 shall only sign using Private Keys where the corresponding Public Keys have been incorporated in Organisation Certificates with the corresponding Remote Party Role.

Object to which signature relates	Party Digitally Signing	Required Remote Party Role in the Certificate used to check signature
Commissioning Outcome File	Commissioning Party	commissioningPartyFileSigning
Migration Common File	Requesting Party	requestingPartyFileSigning
Migration Group File	Requesting Party	requestingPartyFileSigning
Migration Group Encrypted File	Requesting Party	requestingPartyFileSigning
Migration Common Validation File	S1SP	s1SPMigrationSigning
S1SP Commissioning File	S1SP	s1SPMigrationSigning
XML documents created to comply with the DUIS Schema	Commissioning Party	commissioningPartyXmlSigning

Table 5.5

Counters

5.6 Each Requesting Party, each S1SP and the Commissioning Party shall maintain counters, which are sequentially increased for each file created, according the requirements of Table 5.7 so that the files each creates shall, except in cases of replay, pass the anti-replay checks specified in Table 5.9.

5.7 Where an entity acts as the Authenticator with respect to the checks and processing required by Table 5.9, it shall have the capacity to establish and maintain the counters in the 'Counter of Authenticator' column of Table 5.7 in the way required by Table 5.9.

File Type	Party creating the file	Counter of file creator	Counter of Authenticator
Commissioning Outcome File	Commissioning Party	Commissioning Outcome File Counter	Commissioning Outcome File Stored Counter
Migration Common File	Requesting Party	Migration Common File Counter. For clarity, this counter shall be included, along with RequestingPartyID, in all files related to this Migration Common File. Other counters shall additionally be included in all such related files.	Migration Common File Stored Counter
Migration Group File	Requesting Party	Migration Group File Counter	Migration File Group Stored Counter
Migration Group Encrypted File	Requesting Party	Migration Group Encrypted File Counter	Migration File Group Encrypted Stored Counter
Migration Common Validation File	S1SP	Migration Common Validation File Counter	Migration File Common Validation Stored Counter
S1SP Commissioning File	S1SP	S1SP Commissioning File Counter	S1SP Commissioning File Stored Counter

Table 5.7

Creation and validation of standard information

5.8 Before the Migration of any set of SMETS1 Installations is triggered pursuant to Clause 5.12, the Requesting Party shall create, populate with details of that set of SMETS1 Installations, Digitally Sign and then submit to the DCC a Migration Common File adhering to 'Migration Common File Device Selection Requirements' for the specific GroupID, as specified in the Group Specific Requirements. The Requesting Party shall not include in any Migration Common File details for any Active Device where either the CriticalSupplierCertificateID or NonCriticalSupplierCertificateID have the null value. The Requesting Party may only set the ToBeCommissionedByDCC to be False where the Migration Common File only contains details on Active Devices.

The Requesting Party shall set ToBeCommissionedByDCC to 'True' unless:

(i) all of the Devices that form such a SMETS1 Installation are Active Devices; and

(ii) the Responsible Supplier (or a Responsible Supplier to which it is Affiliated) has indicated, pursuant to Clause 4.35 (b), that it wishes to carry out the steps to commission all such Devices; and

(iii) all Supplier Certificate IDs within the file refer to Certificates all of which contain User IDs allocated to the same Supplier Party (or allocated to multiple Supplier Parties provided that they are all Affiliates of one another).

5.9 Where the DCC receives a Migration Common File, the DCC shall, as the Authenticator, undertake, using whichever parts of the DCC Live Systems it chooses, the sequence of checks and processing required by Table 5.9 for such a file.

Step number	**Checks and processing**
	Should any of the following checks fail, the Authenticator shall cease processing that file, discard it and raise an Incident.
5.9.1	Confirm the xml file is well formed and valid against the SMETS1 Migration Schema and meets the requirements of Clause 10.1
5.9.2	Check Cryptographic Protection in terms of the signature within the file
5.9.3	Confirm the Remote Party Role specified in the Certificate which was used to Check Cryptographic Protection at Step Number 2 aligns to that required by Table 5.5 for the relevant file type
5.9.4	Confirm Validity of the Certificate used to Check Cryptographic Protection at Step Number 2
5.9.5	Where the file is a Migration Common File confirm either that: 1. the Authenticator holds one or more Migration Common File Stored Counters for the Requesting Party Identifier (RequestingPartyID) and the MCFCounter is not equal to any such Migration Common File Stored Counter created in the last 60 days; or 2. the Authenticator does not hold any Migration Common File Stored Counter for this Requesting Party Identifier Should this check succeed, the Authenticator shall: 1. Create a Migration Common File Stored Counter that is set to the value of MCFCounter
5.9.6	Where the file is a Migration Group File confirm either that: 1. the Authenticator holds one or more Migration Group File Stored Counters for this Requesting Party Identifier (RequestingPartyID) and the MGFCounter is not equal to any such Migration Group File Stored Counter created in the last 60 days; or 2. the Authenticator does not hold a Migration Group File Stored Counter for this Requesting Party Identifier (RequestingPartyID) Should this check succeed, the Authenticator shall: 1. Create a Migration Group File Stored Counter that is set to the value of MGFCounter.
5.9.7	Where the file is a Migration Group Encrypted File confirm either that: 1. the Authenticator holds one or more Migration Group Encrypted File Stored Counters for this Requesting Party Identifier (RequestingPartyID) and the MEFCounter is not equal to any such Migration Group Encrypted File Stored Counter created in the last 60 days; or 2. the Authenticator does not hold a Migration Group Encrypted File Stored Counter for this Requesting Party Identifier (RequestingPartyID) Should this check succeed, the Authenticator shall: 1. Create a Migration Group Encrypted File Stored Counter that is set to the value of MEFCounter.
5.9.8	Where the file is a Migration Common Validation File confirm either that: 1. the Authenticator holds one or more Migration File Common Validation Stored Counters for this Requesting Party Identifier (RequestingPartyID) and the MVFCounter is not equal to any such Migration File Common Validation Stored Counter created in the last 60 days; or 2. the Authenticator does not hold a Migration File Common Validation Stored Counter for this Requesting Party Identifier (RequestingPartyID) Should this check succeed, the Authenticator shall: 1. Create a Migration File Common Validation Stored Counter that is set to the value of MVFCounter.

Step number	Checks and processing
5.9.9	Where the file is a S1SP Commissioning File confirm either that: 1. the Authenticator holds one or more S1SP Commissioning File Stored Counters for this S1SP Identifier (S1SPID) and the SCFCounter is not equal to any such S1SP Commissioning File Stored Counter created in the last 60 days; or 2. the Authenticator does not hold a S1SP Commissioning File Stored Counter for this S1SP Identifier (S1SPID) Should this check succeed, the Authenticator shall: 1. Create a S1SP Commissioning File Stored Counter that is set to the value of SCFCounter.
5.9.10	NOT USED.

Table 5.9

5.10 Where all checks and processing at Clause 5.10 succeed for a Migration Common File, the DCC shall, using whichever parts of the DCC Live Systems it chooses:

(a) ensure that the file is provided to the relevant S1SP, the relevant DCO, and, where 'ToBeCommissionedByDCC' is set to 'True', the Commissioning Party and, where 'ToBeCommissionedByDCC' is set to 'False', the Responsible Supplier for the SMETS1 Installations identified with that file over the SMETS1 Migration Interface subject to the naming requirement at Clause 10.2;

(b) create a Migration Common Validation File with the Migration Header having the same values as that of the Migration Common File;

(c) for each SMETS1Installation detailed in the Migration Common File, add a SMETS1Installation element to the Migration Common Validation File where the DeviceID element within the CHF element is that of the SMETS1 CHF of the SMETS1 Installation, and undertake the full sequence of checks and processing in Table 5.10. Should one of those checks fail for a SMETS1 Installation, the DCC shall append to the SMETS1Installation element, a FailedCheck element which includes (1) the relevant StepNumber from Table 5.10 (the 'FailedStepNumber') and (2) the SupportingData (as required by the relevant row in from Table 5.10). For clarity, the DCC shall undertake all checks from Table 5.10 for the SMETS1 Installation and so there may be zero, one or many FailedCheck elements for a SMETS1Installation element; and

(d) once all checks are completed for all SMETS1 Installations in the Migration Common File, Digitally Sign the Migration Common Validation File, ensure the relevant S1SP and the relevant DCO has that file, and send that file to the Requesting Party identified by RequestingPartyID.

StepNumber	Check and processing	SupportingData
5.10.1	For the CHF then the ESME then the GSME (if present) and then the PPMID (if present), confirm that the DeviceDetail specified equates to at least one entry on the Central Products List and that that CPL entry is for the required DeviceType	DeviceID of the Device whose Device Model is not on the CPL

StepNumber	Check and processing	SupportingData
5.10.2	For the CHF then the ESME then the GSME (if present) and then the PPMID (if present), confirm that the DeviceDetail specified is one allowable for the GroupID according to the Group Device Model Combination List.	DeviceID of the Device whose Device Model is not within the Group specified by the GroupID
5.10.3	Confirm there is at least one entry on the SMETS1 Eligible Product Combinations which has the combination of Device Models and Device Types specified for this SMETS1 Installation in relation to its CHF, ESME, GSME (if present) and PPMID (if present) and, for at least one such entry the GroupID matches the GroupID in the file.	None
5.10.4	For the CHF then the GPF then the ESME then the GSME (if present) then the PPMID (if present) then the IHD (if present) then the CAD (if present), confirm that DeviceID is not already recorded for any Device in the Smart Metering Inventory.	DeviceID of the Device which is already recorded in the Smart Metering Inventory.
5.10.5	Except for any where the value of CertificateID is the Null Certificate ID, for the ESME, Confirm Validity of each of the Certificates identified by each of the associated four CertificateIDs.	CertificateID for the invalid Certificate
5.10.6	Except for any where the value of CertificateID is the Null Certificate ID, for the GPF, Confirm Validity of each of the Certificates identified by each of the associated four CertificateIDs.	CertificateID for the invalid Certificate
5.10.7	Except for any where the value of CertificateID is the Null Certificate ID, for the GSME if present, Confirm Validity of each of the Certificates identified by each of the associated two CertificateIDs.	CertificateID for the invalid Certificate
5.10.8	Unless the value of the CriticalSupplierCertificateID is the Null Certificate ID for the ESME, confirm, using the Certificates identified by the ESME's CriticalSupplierCertificateID and NonCriticalSupplierCertificateID: • Neither the Critical Supplier ID nor the Non-Critical Supplier ID has the null value; and • the Critical Supplier ID and the Non-Critical Supplier ID identify the same Supplier Party (which is referred to as the 'ESME Supplier Party' in later steps in this Table).	CriticalSupplierCertificateID || NonCriticalSupplierCertificateID
5.10.9	Unless the value of the CriticalSupplierCertificateID is the Null Certificate ID for the ESME, confirm, that, according to Registration Data, the 'ESME Supplier Party' is the current Import Supplier in relation to the MPxN specified in the ESME element.	CriticalSupplierCertificateID
5.10.10	Unless the value of the CriticalSupplierCertificateID is the Null Certificate ID for the ESME, confirm, that, according to Registration Data, there is no change within the next 7 days to the Import Supplier in relation to the MPxN specified in the ESME element.	
5.10.11	Unless the value of the CriticalNetworkOperatorCertificateID is the Null Certificate ID for the ESME, confirm, using the Certificates identified by the ESME's CriticalNetworkOperatorCertificateID and NonCriticalNetworkOperatorCertificateID: • Neither the Critical Network Operator ID nor the Non-Critical Network Operator ID has the null value; and • the Critical Network Operator ID and the Non-Critical Network Operator ID identify the same Network Party (which is referred to as the 'ESME Network Party' in later steps in this Table).	CriticalNetworkOperatorCertificateID || NonCriticalNetworkOperatorCertificateID:
5.10.12	Unless the value of the CriticalNetworkOperatorCertificateID is the Null Certificate ID for the ESME, confirm, that, according to Registration Data, the 'ESME Network Party' is the current Electricity Distributor in relation to the MPxN specified in the ESME element.	CriticalNetworkOperatorCertificateID
5.10.13	If GSME is present, unless the value of the CriticalSupplierCertificateID is the Null Certificate ID for the GSME, confirm, using the Certificates identified by the GSME's CriticalSupplierCertificateID, the GSME's NonCriticalSupplierCertificateID, the GPF's CriticalSupplierCertificateID, and the GPF's NonCriticalSupplierCertificateID: • Neither the Critical Supplier IDs nor the Non-Critical Supplier IDs have the null value; and • the Critical Supplier IDs and the Non-Critical Supplier IDs identify the same Supplier Party (which is referred to as the 'Gas Supplier Party' in later steps in this Table).	CriticalSupplierCertificateID || NonCriticalSupplierCertificateID
5.10.14	Unless the value of the CriticalSupplierCertificateID is the Null Certificate ID for the GSME, confirm, that, according to Registration Data, the 'Gas Supplier Party' is the Gas Supplier in relation to the MPxN specified in the GSME element.	CriticalSupplierCertificateID
5.10.15	Unless the value of the CriticalSupplierCertificateID is the Null Certificate ID for the GSME, confirm, that, according to Registration Data, there is no change within the next 7 days to the Gas Supplier in relation to the MPxN specified in the GSME element.	

StepNumber	Check and processing	SupportingData
5.10.16	Unless the value of the CriticalNetworkOperatorCertificateID is the Null Certificate ID for the GPF, confirm, using the Certificates identified by the GPF's CriticalNetworkOperatorCertificateID and NonCriticalNetworkOperatorCertificateID: • Neither the Critical Network Operator ID nor the Non-Critical Network Operator ID has the null value; and • the Critical Network Operator ID and the Non-Critical Network Operator ID identify the same Network Party (which is referred to as the 'Gas Network Party' in later steps in this Table).	CriticalNetworkOperatorCertificateID || NonCriticalNetworkOperatorCertificateID:
5.10.17	Unless the value of the CriticalNetworkOperatorCertificateID is the Null Certificate ID for the GPF, confirm, that, according to Registration Data, the Gas Network Party is the Gas Transporter in relation to the MPxN specified in the GSME element.	CriticalNetworkOperatorCertificateID
5.10.18	For each of the IHD and CAD, confirm the DeviceType element within the DeviceDetail has the required value.	DeviceID of the Device.

Table 5.10

5.11 Where the Requesting Party, the S1SP or the DCO receives a Migration Common Validation File, it shall, as the Authenticator, undertake the sequence of checks and processing required by Table 5.9 for such a file.

<u>Preparing to trigger Migration</u>

5.12 Where a Requesting Party wishes to Migrate one or more SMETS1 Installations (the 'Requested Installations'), and is in receipt of the required Migration Authorisations for the Requested Installations (or is deemed to have received them pursuant to Clause 4.26(a) or the definition of Migration Authorisation), the Requesting Party shall first:

(a) confirm a Migration Common File including the Requested Installations has been submitted to the DCC and authenticated as required by Clause 5.8, and a corresponding Migration Common Validation File has been received within the prior 24 hours and authenticated as required by Clause 5.11;

(b) confirm that in the Migration Common Validation File, no errors were detailed for the Requested Installations;

(c) confirm that there has been one or more wide area network communications with the Communications Hub in each of the Requested Installations within the last 7 days;

(d) where the relevant SMSO is reasonably aware that the Responsible Supplier (or, in the case of Dormant Meters and any associated Devices within the same SMETS1 Installation for which the same Supplier Party is the Responsible Supplier, the DCC) intends to configure any Device within any Requested Installation in accordance with the requirements of the SMETS1 Supporting Requirements (in whole or in part), check that the SMETS1 SMSO has sent the necessary instructions to all such Devices within the Requested Installations to give effect to such configuration;

(e) arrange for the SMETS1 SMSO to take the necessary steps to ensure that all Devices within the Requested Installations, and any associated systems, have been configured in line with the requirements notified by the DCC pursuant to Clause 5.1(b) and where such steps are required, confirm that such steps have been undertaken; and

(f) if required by the 'Migration Group File' section of this TMAD for the specified GroupID, populate a Migration Group File with details for the Requested Installations required for the specified GroupID, Digitally Sign and then submit it to the DCC, with the Migration Header having the same values as the Migration Common File; and

(g) if required by the 'Migration Group Encrypted File' section of this TMAD for the specified GroupID, populate with details for the Requested Installations, Digitally Sign and then submit to the DCC, a Migration Group Encrypted File, with the Migration Header having the same values as the Migration Common File. The EncryptedS1SPGroupInformation and MasterKeyInformation parts of a Migration Group Encrypted File shall be encrypted according to Clause 11 where the Public Keys used are those notified by the DCC pursuant to Clause 5.1(a) for the GroupID in question.

S1SP and DCO receipt of migration data

5.13 Where the DCC receives a Migration Group Encrypted File, the DCC shall ensure that the DCO and the S1SP, corresponding to the GroupID in the file, have that file.

5.14 Where the DCC receives a Migration Group File, the DCC shall ensure the S1SP corresponding to the GroupID in the file, has that file.

DCO processing on receipt of migration data

5.15 Where the DCO receives a Migration Group Encrypted File, the DCO shall, as the Authenticator, undertake the sequence of checks and processing required by Table 5.9 for such a file. The DCO shall then:

(a) attempt to decrypt the MasterKeyInformation parts of the Migration Group Encrypted File according to Clause 11, where the Public Keys used are those published by DCC pursuant to Clause 5.1(a) for the GroupID in question; and

(b) if this step fails, the DCO shall cease processing that file, discard it and raise an Incident.

5.16 When the DCO has authenticated a Migration Group Encrypted File, it shall start a timer. If that timer reaches 48 hours without the S1SP requesting use of any details in that file, the DCO

shall discard the file.

5.17 Where the S1SP requests that the DCO uses details in a Migration Group Encrypted File before the 48 hour timer has elapsed, the DCO shall start another timer. When that timer reaches 60 days, the DCO shall discard any details in the Migration Group Encrypted File related to SMETS1 Installations for which the S1SP has not requested any details be used by the DCO.

5.18 When the DCO authenticates the first Migration Common Validation File for a specific DCO Required File Set, pursuant to Clause 5.20, it shall start a timer. If that timer reaches 24 hours without all of the DCO Required File Set being received, the DCO shall discard the files it has received in that DCO Required File Set.

5.19 If and only if the DCO receives all of the files in the DCO Required File Set before its corresponding timer reaches 24 hours, it shall identify the set of SMETS1 Installations from that set which it will allow to be processed further (the "**DCO Viable Installations**"). The DCO shall include in the DCO Viable Installations for this DCO Required File Set all the SMETS1 Installations which:

(a) are included in the Migration Common Validation File, the Migration Common File and, if required, the Migration Group Encrypted File;

(b) do not have any FailedCheck elements within the corresponding SMETS1Installation element in the Migration Common Validation File; and

(c) have not failed any of the checks applied by the DCO as required by 'DCO Migration Group Encrypted File data validation' for the specified GroupID, as detailed in the Group Specific Requirements.

5.20 Where the S1SP requests that the DCO uses some details in relation to a SMETS1 Installation, the DCO shall respond to such requests notifying the S1SP of an error unless either:

(a) the SMETS1 Installation is one of the installations in a set of DCO Viable Installations for which the DCO holds the corresponding DCO Required File Set; or

(b) the SMETS1 Installation was one of the installations in a set of DCO Viable Installations for which the DCO held the corresponding DCO Required File Set when it received a notification from the S1SP that the CHF forming part of that SMETS1 Installation was commissioned.

5.21 When processing such requests from the S1SP, the DCO shall treat only information which is (1) for a DCO Viable Installation and (2) in the corresponding Migration Group Encrypted File

as Authorised DCO SMETS1 Device Credentials.

S1SP processing on receipt of migration data

5.22 Where the S1SP receives a Migration Common File, a Migration Common Validation File, a Migration Group File or a Migration Group Encrypted File, the S1SP shall, as the Authenticator, undertake the sequence of checks and processing required by Table 5.9 for such a file.

5.23 For a Migration Group Encrypted File where EncryptedS1SPGroupInformation is required for this GroupID, the S1SP shall then:

(a) attempt to decrypt the EncryptedS1SPGroupInformation parts of the Migration Group Encrypted File according to Clause 11, where the Public Keys used are those notified by DCC pursuant to Clause 5.1(a) for the GroupID in question; and

(b) confirm that the plaintext output from decrypting EncryptedS1SPGroupInformation is well formed and valid against the SMETS1 Migration Schema for a DecryptedS1SPGroupInformation structure.

If either step fails, the S1SP shall cease processing that file, discard it and raise an Incident.

5.24 When the S1SP authenticates, pursuant to Clause 5.22, the first Migration Common Validation File, for a specific S1SP Required File Set, it shall start a timer. If that timer reaches 24 hours without all of the S1SP Required File Set being received, the S1SP shall discard the files it has received in that S1SP Required File Set.

5.25 Where the SISP has received all the files in an S1SP Required File Set and has successfully undertaken the checks required by Clause 5.20 in relation to each of the files, the S1SP shall undertake the sequence of checks and processing required by Table 5.25. Where a SMETS1 Installation fails any of those checks, the S1SP shall include details of that SMETS1 Installation's failure in an S1SP Commissioning File and the S1SP shall undertake no further processing in relation to such SMETS1 Installations as part of the processing of that Migration Group File. Only the SMETS1 Installations which pass all of the checks in Table 5.25 shall be included in the set of S1SP Viable Installations for the S1SP Required File Set.

Step number	Check and processing
	Should any of the following checks fail, checking in relation to that SMETS1 Installation shall cease
5.25.1.1	For each CHFIdentifier in the Migration Group File, where one is required for this GroupID, or in the Migration Group Encrypted File, where a Migration Group File is not required for this GroupID, confirm that the Migration Common File contains a CHFIdentifier with the same value

Step number	Check and processing
5.25.1.2	For each CHFIdentifier in the Migration Group File, where one is required for this GroupID, or in the Migration Group Encrypted File, where a Migration Group File is not required for this GroupID, confirm that the Migration Common Validation File does not contain a CHFIdentifier with the same value indicating a validation error
5.25.2.X	Undertake the steps required by the 'S1SP Migration Group File data validation' section of this TMAD for the specified GroupID, where X is the Step number value specified in that section
5.25.3.X	Undertake the steps required by the 'S1SP Migration Group Encrypted File data validation' section of this TMAD for the specified GroupID, where X is the Step number value specified in that section

Table 5.25

5.26 The S1SP shall treat only information which is (i) for an S1SP Viable Installation and (ii) in the corresponding Migration Group Encrypted File as Authorised S1SP SMETS1 Device Credentials.

5.27 For each of the S1SP Viable Installations, the S1SP, and where required the DCO, shall:

(a) undertake, in the order specified, the checks and processing required by the 'S1SP / DCO Commissioning of SMETS1 Installation' section of this TMAD for the associated GroupID;

(b) where a SMETS1 Installation fails any of those checks or processing which is flagged as 'Critical':

(i) include details of that SMETS1 Installation's failure in an S1SP Commissioning File;

(ii) where steps are specified at 'Installation Rollback' for this GroupID, undertake the steps specified to allow communications with the SMETS1 Installation via the relevant SMETS1 SMSO; and

(iii) undertake no further processing in relation to that SMETS1 Installation as part of the processing of the 'DCO Required File Set' or 'S1SP Required File Set', and discard information it has stored or derived about that SMETS1 Installation; and

(c) where a SMETS1 Installation completes all checks and processing without any failures flagged as 'Critical':

(i) record or derive all the information it requires in order to maintain communications with the CHF which forms part of that SMETS1 Installation; and

(ii) include details of that SMETS1 Installation's success in an S1SP Commissioning File.

5.28 The S1SP may include details relating to one or more SMETS1 Installations in each S1SP Commissioning File subject to that inclusion not delaying the sending of details related to any one SMETS1 Installation by more than 60 minutes. Whenever the S1SP creates an S1SP Commissioning File, it shall Digitally Sign that file and send that file:

(a) to the Requesting Party identified by RequestingPartyIdentifier; and either:

(b) where, in the corresponding Migration Common File, the 'ToBeCommissionedByDCC' is set to 'True', to the Commissioning Party identified by CommissioningPartyIdentifier; or

(c) where, in the corresponding Migration Common File, the 'ToBeCommissionedByDCC' is set to 'False', to the Responsible Supplier for the Devices referred to in that file over the SMETS1 Migration Interface.

6 Commissioning Requirements

6.1 Where the Commissioning Party receives a Migration Common File or an S1SP Commissioning File, then the Commissioning Party shall, as the Authenticator, undertake the sequence of checks and processing required by Table 5.9 for such a file. Additionally, the Commissioning Party shall check that any Migration Common File has a value for 'ToBeCommissionedByDCC' set to 'True'. If this check fails, the Commissioning Party shall discard the file and cease processing of it.

6.2 Where the checks undertaken pursuant to Clause 6.1 are successful and the file is a Migration Common File, the Commissioning Party shall start a timer. When that timer reaches 60 days or the Commissioning Party has received and processed S1SP Commissioning Files for all SMETS1 Installations in the Migration Common File, the Commissioning Party shall discard the Migration Common File.

6.3 Where the checks undertaken pursuant to Clause 6.1 are successful and the file is an S1SP Commissioning File, the Commissioning Party shall, in the following sequence:

(a) confirm that it holds a Migration Common File where the Migration Header has the same values as that S1SP Commissioning File. If it does not, processing of the S1SP Commissioning File shall cease, the file shall be discarded and an Incident shall be raised;

(b) confirm that the S1SP Commissioning File contains details of at least one SMETS1 Installation which the S1SP has successfully processed. If it does not, processing of the S1SP Commissioning File shall cease and the file shall be discarded;

(c) for each SMETS1 Installation specified as being successful in the S1SP Commissioning File, confirm that there is a corresponding SMETS1 Installation in the Migration Common File. Should this check fail for any SMETS1 Installation, processing of the S1SP Commissioning File shall cease, the file shall be discarded and an Incident shall be raised; and

(d) for each SMETS1 Installation in each S1SP Commissioning File that successfully passes the checks at Clauses 6.3(a), 6.3(b) and 6.3(c):

(i) submit the Commissioning Requests to the DCC, in line with the requirements of Clause 8 (where 'Target SMETS1 Device', 'Other SMETS1 Device' and 'RemotePartyRole' have their Table 6.3 values for the relevant Commissioning Request), as required by Table 6.3 in the sequence specified, using the details from the Migration Common File for that SMETS1 Installation; and

(ii) include details of that SMETS1 Installation's processing in a Commissioning Outcome File, specifically by including a SMETS1Installation element, where the DeviceID element within the CHF element is that of the SMETS1 CHF of the SMETS1 Installation. Additionally, where there are any errors in relation to 'StepNumbers' 6.3.1 to 6.3.20 the Commissioning Party shall append to the SMETS1Installation element, a FailedCheck element which includes the relevant StepNumber from Table 6.3 (the 'FailedStepNumber'). For clarity (1) the Commissioning Party shall undertake all relevant steps required by Table 6.3 for the SMETS1 Installation and so there may be zero, one or many FailedCheck elements for a SMETS1Installation element; and (2) where the relevant CertificateID is null or a Device is not present, a step cannot produce errors.

StepNumber	Commissioning Request	Only submit if:	Target SMETS1 Device ID	Other SMETS1 Device ID	RemotePartyRole
6.3.1	Device Pre-notification	True	DeviceID in ESME	NA	NA
6.3.2	Update HAN Device Log	True	DeviceID in CHF	DeviceID in ESME	NA
6.3.3	Device Pre-notification	If GSME present	DeviceID in GSME	NA	NA
6.3.4	Update HAN Device Log	If GSME present	DeviceID in CHF	DeviceID in GSME	NA
6.3.5	Device Pre-notification	If PPMID present	DeviceID in PPMID	NA	NA
6.3.6	Update HAN Device Log	If PPMID present	DeviceID in CHF	DeviceID in PPMID	NA
6.3.7	Device Pre-notification	If IHD present	DeviceID in IHD	NA	NA
6.3.8	Update HAN Device Log	If IHD present	DeviceID in CHF	DeviceID in IHD	NA
6.3.9	Device Pre-notification	If CAD present	DeviceID in CAD	NA	NA
6.3.10	Update HAN Device Log	If CAD present	DeviceID in CHF	DeviceID in CAD	NA
6.3.11	Request Handover Of DCC Controlled Device	If Supplier Certificate IDs in the ESME element are not null	DeviceID in ESME	NA	Supplier
6.3.12	Request Handover Of DCC Controlled Device	If (GSME present) and (Supplier Certificate IDs in the GSME element are not null)	DeviceID in GSME	NA	Supplier
6.3.13	Commission Device	True	DeviceID in ESME	NA	NA

StepNumber	Commissioning Request	Only submit if:	Target SMETS1 Device ID	Other SMETS1 Device ID	RemotePartyRole
6.3.14	Commission Device	If GSME present	DeviceID in GSME	NA	NA
6.3.15	Join Service (Non-Critical)	If PPMID present	DeviceID in PPMID	DeviceID in ESME	NA
6.3.16	Join Service (Critical)	If PPMID present	DeviceID in ESME	DeviceID in PPMID	NA
6.3.17	Join Service (Non-Critical)	If GSME present	DeviceID in GSME	DeviceID in GPF	NA
6.3.18	Request Handover Of DCC Controlled Device	If (GSME present) and (Supplier Certificate IDs in the GPF element are not null)	DeviceID in GPF	NA	Supplier
6.3.19	Request Handover Of DCC Controlled Device	If Network Operator Certificate IDs in the ESME element are not null	DeviceID in ESME	NA	NetworkOperator
6.3.20	Request Handover Of DCC Controlled Device	If Network Operator Certificate IDs in the GPF element are not null	DeviceID in GPF	NA	NetworkOperator

Table 6.3

6.4 The Commissioning Party may include details relating to one or more SMETS1 Installations in each Commissioning Outcome File subject to that inclusion not delaying the sending of details related to any one SMETS1 Installation by more than 60 minutes and, where a Supplier Party is identified in the corresponding entries in the Migration Common File, the Supplier Party is the Responsible Supplier for at least one of the Smart Meters in all of the SMETS1 Installations in that file. Whenever the Commissioning Party creates a Commissioning Outcome File, it shall:

(a) ensure the Migration Header has the same values as that of the Migration Common File; and

(b) Digitally Sign that file and send that file to:

(i) the Requesting Party identified by RequestingPartyIdentifier; and

(ii) where one or more Supplier Parties is identified in the corresponding entries in the Migration Common File, each such Supplier Party via the SMETS1 Migration Interface.

6.5 Where an S1SP receives a Commissioning Request that in accordance with, and subject to, Clause 8.1 is to be treated as a 'Commission Device' Service Request (with its DUIS meaning) for a Device communicating via a CHF that it has established communication with pursuant to Clause 5.27, the S1SP shall establish that Device's Device Model using the Smart Metering Inventory and undertake the processing required for such a Device Model according to the S1SP requirements in the SMETS1 Supporting Requirements. Upon successful completion of the required S1SP processing, where the relevant Service Request is a Commissioning Request, the S1SP shall issue an S1SP Alert, populated according to Table 6.5. For clarity, S1SP Alerts are defined in Version 3.0 of the DCC User Interface Specification, therefore a User that has

not yet sent a Service Request using Version 3.0 of the DUIS XML Schema shall not receive such S1SP Alerts.

DUIS Data Item	Value
RequestID	Shall be the concatenation of: • The Notified Critical Supplier ID, where the S1SP holds such an identifier in relation to the Device or, where the S1SP does not hold such an identifier, a User ID associated with the Responsible Supplier for the Device; • The Business Target ID in the Commissioning Request; and • 1, separated by ":".
DeviceID	The Business Target ID in the Commissioning Request
S1SPAlertCode	S1MC1
AdditionalInformation	Shall be the sequential concatenation of the following data items: • the MPxN that is, according to the Smart Metering Inventory, associated with the Device identified by the DeviceID; • the EUI-64 identifier of the Communications Hub Function associated with the Device identified by the DeviceID; and • only where the Device identified by the DeviceID is a Gas Smart Meter, the EUI-64 identifier of the Gas Proxy Function associated with that Gas Smart Meter; with a colon (":") used a separator between each data item in the concatenation.
DateTime	Any value as set out in Clause 3.9.15.2 in the DCC User Interface Specification
ds: Signature	Any value as set out in Clause 3.9.15.2 in the DCC User Interface Specification

Table 6.5

6.6 Where, in a Migration Common File, the 'ToBeCommissionedByDCC' set to 'False' the Responsible Supplier for the Devices referred to in that file shall undertake those steps necessary (including submitting Service Requests) to achieve an outcome that is equivalent to that which would have been achieved had the Commissioning Party carried out the steps set out in the Clause 6 in relation to those Devices.

6.7 The S1SP for GroupID = "DA" shall not process any request, received via its interface with the SMETS1 SMSO for that GroupID, to communicate with or generate instructions for a Device in relation to which the steps in Clause 5.12(e) have been carried out, except pursuant to Clause 3.14D.

7 Decommissioning of a Requesting Party or the Commissioning Party

7.1 The DCC shall develop a timetable that sets out the dates (each a proposed "**RP Decommissioning Date**") at which it proposes to decommission each Requesting Party, this timetable being a draft of the "**RP Decommissioning Timetable**".

7.2 The date within the draft timetable upon which it is proposed to decommission any particular Requesting Party shall be no earlier than twelve months after the date upon which the SMETS1

Eligible Product Combinations is updated by the DCC so as to include an entry for each of the Device Model combinations contained within each Group that pertains to that Requesting Party.

7.3 The DCC shall develop and consult on the RP Decommissioning Timetable and submit it to the Secretary of State for approval in accordance with the following process:

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

(b) where a disagreement arises with any Supplier Party with regard to any proposal as to the content of the document, the DCC shall endeavour to reach an agreed proposal with that person consistent with the purposes of the RP Decommissioning Timetable;

(c) the DCC shall send a draft of the RP Decommissioning Timetable to the Secretary of State as soon as is practicable after completion of the process described in (a) and (b) above, and shall when doing so provide to the Secretary of State:

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

(ii) copies of the consultation responses received; and

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

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

7.4 Following approval of the RP Decommissioning Timetable by the Secretary of State in accordance with Clause 7.3, the DCC shall publish the RP Decommissioning Timetable to all Supplier Parties and send a copy of the final document to the Secretary of State and to the Authority.

7.5 The DCC may update the RP Decommissioning Timetable by following the procedure in Clause 7.3, provided that the DCC must ensure that the most up to date RP Decommissioning Timetable is published to all Supplier Parties and a copy is provided to the Secretary of State and to the Authority.

7.6 Following the expiry of the RP Decommissioning Date for a Requesting Party, the DCC shall

ensure that that Requesting Party does not take any further step under this Code that could result in, or contribute towards, the Migration of any SMETS1 Installation.

7.7 As soon as reasonably practicable following the RP Decommissioning Date for a Requesting Party, the DCC shall submit a Certificate Revocation Request for all Organisation Certificates in which:

(a) that Requesting Party is identified by the Entity Identifier of the subject of that Organisation Certificate; and

(b) any S1SP that pertains to any Group that pertains to that Requesting Party is identified by the Entity Identifier of the subject of that Organisation Certificate and where such Organisation Certificates have a Remote Party Role of 's1SPMigrationSigning'.

7.8 The DCC shall, as soon as reasonably practicable following the revocation of each of the Organisation Certificates referred to in Clause 7.7, destroy the Private Key associated with each such Organisation Certificate and any associated cryptographic material.

7.9 The DCC shall as soon as reasonably practicable after the RP Decommissioning Date for a Requesting Party:

(a) destroy any Secret Key Material in addition to that referred to in Clause 7.7;

(b) revoke any Certificate associated with any other Public Key in addition to those referred to in Clause 7.7; and

(c) delete any Data, that (in each case) is held within any part of the DCC Systems and that was used (or was intended for use) for the purpose of the Migration of the SMETS1 Installations that pertained to that Requesting Party and that is not required for the purposes of providing ongoing Services under the Code in relation to the Devices comprising those SMETS1 Installations; provided that Migration Authorisations may be retained for a limited period of time in order to resolve any disagreements over the process.

7.10 As soon as reasonably practicable following the last RP Decommissioning Date the DCC shall submit a Certificate Revocation Request for all Organisation Certificates that identify the Commissioning Party by the Entity Identifier of the subject of those Organisation Certificates.

7.11 The DCC shall, as soon as reasonably practicable following the revocation of each of the Organisation Certificates referred to in Clause 7.10, destroy the Private Key associated with each such Organisation Certificate and any associated cryptographic material.

7.12 The DCC shall as soon as reasonably practicable after the last RP Decommissioning Date:

(a) destroy any Secret Key Material in addition to that referred to in Clause 7.10;

(b) revoke any Certificate associated with any other Public Key in addition to those referred to in Clause 7.10; and

(c) delete any Data,

that (in each case) is held within any part of the DCC Systems and that was used (or was intended for use) for the purpose of the operation of the Commissioning Party; provided that information sent to Supplier Parties may be retained for a limited period of time in order to resolve any disagreements over the process.

7.13 The DCC shall as soon as reasonably practicable following the decommissioning of any Requesting Party or the Commissioning Party, obtain an independent audit and provide to the SMKI PMA the report of that audit, confirming that the decommissioning has been properly and successfully carried out together with any remediation plan that may be required.

7.14 Prior to the decommissioning of the Requesting Party, the DCC shall apply the configurations as required by 'Post Migration Configuration' for the specified GroupID.

8 Commissioning Requests

8.1 The Commissioning Party and the DCC shall process Commissioning Requests as if they were Service Requests except as varied in this Clause 8.

8.2 The DCC shall not apply any checks on Commissioning Requests that relate to User Role.

8.3 The DCC shall not apply any checks on Commissioning Requests that validate the Notified Critical Supplier ID (with its SMETS1 Supporting requirements meaning) against the Business Originator ID (with its DUIS meaning).

8.4 The DCC shall not apply any validation to Commissioning Requests that relate to Registration Data unless such validation is required by this Clause 8.

8.5 The Commissioning Party shall populate the data items in all Commissioning Requests according to Table 8.7.4, using the information from the Migration Common File where required. Where the S1SP receives a Countersigned Service Request which has InstallCode set to '00000000000000000000000000000000', the S1SP shall not take any related action which

would or could affect the communications on any HAN.

8.6 The DCC shall apply the validation checks in Table 8.7.1 to all Commissioning Requests that it receives from the Commissioning Party, and shall additionally apply the validation checks in Table 8.7.3 to any Commissioning Request that it receives from the Commissioning Party which is of the type specified in that Table, and the Commissioning Party shall construct Commissioning Requests accordingly. Where one of the checks required by this Clause 8.6 fails, the DCC shall send a Service Response to the Commissioning Party detailing the relevant Response Code, which shall be interpreted according to Table 8.7.1 or Table 8.7.3 as appropriate to the Response Code. Where the Commissioning Party receives such a Response other than in relation to a 'Request Handover Of DCC Controlled Device', it shall raise an Incident and not continue processing subsequent Commissioning Requests for that SMETS1 Installation until and unless that incident is resolved so as to allow the erroneous requests to be processed without error. Where the Commissioning Party receives such as Response in relation to a 'Request Handover Of DCC Controlled Device', it shall take the actions required by Clause 6.3(d)(ii) and shall continue processing subsequent Commissioning Requests for that SMETS1 Installation.

8.7 The DCC shall apply the checks in Table 8.7.1 and Table 8.7.3 in the sequence they appear in each Table and shall successfully apply all Table 8.7.1 checks before applying checks in Table 8.7.3 . The DCC shall cease processing a Commissioning Request at the point that the first check fails, save that it shall send a response detailing the error to the Commissioning Party.

Validation Check	Response Code	Response Code Name	Response code type	Applicable to response types
The combination of values in the Service Reference and Service Reference Variant fields, with their DUIS meanings, is a combination detailed in one of the rows in Table 8.7.2	E48	Commissioning Party is not allowed to use such Service Requests	Error	Acknowledgement
The Remote Party Role in the Certificate used to verify the Digital Signature on the Commissioning Request is that required by Table 5.5.	C2	Wrong Remote Party Role for Commissioning Request	Error	Acknowledgement
The Business Originator ID in the RequestID (with their DUIS meanings) has the same value as the Entity Identifier in the Certificate used to verify the Digital Signature on the Commissioning Request	E100	Commissioning Party identifier mismatch in Commissioning Service Request	Error	Acknowledgement
Where Business Target ID in the RequestID (with their DUIS meanings) refers to a Device, the Devices is, according to the SMI, a SMETS1 Device or a CAD. For clarity, CADs are not specified in any version of SMETS, and so cannot have an associated SMETS version, where CAD has its DUIS meaning.	C4	Target is not a SMETS1 Device	Error	Acknowledgement
Where the Body part of a Commissioning Request, which is not a 'Device Pre-notification', contains a Device ID (with their DUIS meanings), that Device ID is for a SMETS1 Device according to the Smart Metering Inventory	C5	Other Device is not a SMETS1 Device	Error	Acknowledgement

Table 8.7.1

Commissioning Request name	Service Reference	Service Reference Variant
Request Handover Of DCC Controlled Device	6.21	6.21
Commission Device	8.1	8.1.1
Join Service (Critical)	8.7	8.7.1
Join Service (Non-Critical)	8.7	8.7.2
Update HAN Device Log	8.11	8.11
Device Pre-notification	12.2	12.2

Table 8.7.2

Commissioning Request name	**Validation Check (**With terms having their DUIS meaning, where not defined otherwise)	**Response Code**	**Response Code name**	**Response code type**	**Applicable to response types**
Request Handover Of DCC Controlled Device	If RemotePartyRole is 'supplier' in the Commissioning Request, confirm that the Remote Party Role in all Certificates in ReplacementCertificates is 'supplier'. If RemotePartyRole is 'NetworkOperator' in the request, confirm that the Remote Party Role in all Certificates in ReplacementCertificates is 'networkOperator'.	C062199	Remote Party Role in Certificates different than in request	Error	Acknowledgement
Request Handover Of DCC Controlled Device	Confirm that the Entity Identifiers in all Certificates contained within ReplacementCertificates are identifiers for the same Party.	C062197	Not all identifiers are for the same Party	Error	Acknowledgement
Request Handover Of DCC Controlled Device	If RemotePartyRole is 'Supplier' in the request, confirm that according to: • the Registration Data linking MPxN to current Import Supplier or Gas Supplier, as the context requires; • the MPxN recorded in the Smart Metering Inventory against; the Device identified by Business Target ID in the request; and • the Party identified by the Entity Identifiers in the Certificates, that the Party identified is the current Import Supplier or Gas Supplier for the Device identified.	C062196	Asserted Supplier is not the Supplier	Error	Acknowledgement
Request Handover Of DCC Controlled Device	If RemotePartyRole is 'NetworkOperator' in the request, confirm that according to: • the Registration Data linking MPxN to current Electricity Distributor or Gas Transporter, as the context requires; • the MPxN recorded in the Smart Metering Inventory against; the Device identified by Business Target ID in the request; and • the Party identified by the Entity Identifiers in the Certificates, that the Party identified is the current Electricity Distributor or Gas Transporter for the Device identified.	C062195	Asserted Network Operator is not the Network Operator	Error	Acknowledgement

Table 8.7.3

DUIS Data Item	Commissioning Service Request(s)	Value
Business Originator ID in Request ID	All	A DCC ID allocated by the DCC for use by the Commissioning Party
Business Target ID in Request ID	All except Device Pre-Notification	'Target SMETS1 Device ID'
Business Target ID in Request ID	Device Pre-Notification	A DCC ID allocated by the DCC
Originator Counter in Request ID	Join Service (Critical)	For each 'Target SMETS1 Device ID', a 64-bit unsigned integer with an initial value of 1 that is increased by 1 for each instance of the Commissioning Request
Originator Counter in Request ID	All except Join Service (Critical)	Any value as set out in Clause 5 in SMETS1 Supporting Requirements Document
ExecutionDateTime	All	Never present
RemotePartyRole	Request Handover Of DCC Controlled Device	'Supplier' when processing Certificate IDs provided in relation to a Supplier Party role; or 'NetworkOperator' when processing Certificate IDs provided in relation to a Network Party role; or
RemotePartyFloorSeqNumber	Request Handover Of DCC Controlled Device	0 (zero)
RemotePartyPrepaymentTopUpFloorSeqNumber	Request Handover Of DCC Controlled Device	0 (zero) for RemotePartyRole = 'Supplier' and Device Type = ESME or GSME Otherwise not present.
ReplacementCertificates	Request Handover Of DCC Controlled Device	The Certificates identified by the Certificate IDs specified for this RemotePartyRole
CertificationPathCertificates	Request Handover Of DCC Controlled Device	The Certification Authority Certificates identified in the Certificates included in ReplacementCertificates.
ApplyTimeBasedCPVChecks	Request Handover Of DCC Controlled Device	True
CurrentDateTime	Commission Device	The Commissioning Parties current date-time which shall be within 10 seconds of UTC
TolerancePeriod	Commission Device	0 (zero)
OtherDeviceID	Join Service (Critical) & Join Service (Non-Critical)	'Other SMETS1 Device ID'
DeviceID	Update HAN Device Log	'Other SMETS1 Device ID'
RequestType	Update HAN Device Log	'Add'
JoinTimePeriod	Update HAN Device Log	1 (one)

DUIS Data Item	Commissioning Service Request(s)	Value
ImportMPxN	Update HAN Device Log	For GSME the MPRN specified for the SMETS1 Installation For ESME; the MPAN specified for the SMETS1 Installation.
SecondaryImportMPAN	Update HAN Device Log	Never present
ExportMPAN	Update HAN Device Log	Never present
DeviceID	Device Pre-Notification	'Target SMETS1 Device ID'
DeviceManufacturer	Device Pre-Notification	As specified in relation to the 'Target SMETS1 Device ID'
DeviceModel	Device Pre-Notification	As specified in relation to the 'Target SMETS1 Device ID'
DeviceType	Device Pre-Notification	The device type specified in relation to the 'Target SMETS1 Device ID', so the relevant one of: • ESME • GSME • PPMID • IHD • CAD
SMETSCHTSVersion	Device Pre-Notification	Not present if DeviceType = "CAD'; as specified in the CPL for the Device Model of the Device identified by the 'Target SMETS1 Device ID' otherwise
FirmwareVersion	Device Pre-Notification	As specified in relation to the 'Target SMETS1 Device ID' where present; otherwise omitted from Commissioning Request
ESMEVariant	Device Pre-Notification	Not present unless DeviceType = "ESME'; 'A' otherwise
AssociatedGPFDeviceID	Device Pre-Notification	Never present

Table 8.7.4

8.8 The DCC shall develop and consult on a "Migration Error Handling and Retry Strategy" in accordance with the following process:

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

(b) where a disagreement arises with any Supplier Party with regard to any proposal as to the content of the document, the DCC shall endeavour to reach an agreed proposal with that person consistent with the purposes of the Migration Error Handling and Retry Strategy;

(c) the DCC shall publish a draft of the Migration Error Handling and Retry Strategy as soon as is practicable after completion of the process described in (a) and (b) above together with:

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

(ii) copies of the consultation responses received (apart from those marked confidential); and

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

8.9 Within 14 days of DCC publishing the draft Migration Error Handling and Retry Strategy pursuant to Clause 8.8 any Supplier Party may refer the document to the Secretary of State whose decision on its contents shall be final and binding. In the absence of any such referral, the draft published by the DCC shall be Migration Error Handling and Retry Strategy.

8.10 The Migration Error Handling and Retry Strategy may be updated following the procedure set out in Clause 8.8 and 8.9, provided that the DCC must ensure that the most up to date Migration Error Handling and Retry Strategy is published to all Supplier Parties.

9 SMETS1 Migration Interface

9.1 This Clause 9 specifies the technical interface allowing the exchange of files between the DCC and Supplier Parties pursuant to requirements to exchange files in this TMAD.

9.2 For each Supplier Party, the DCC shall detail directory structures in DCC's Microsoft SharePoint through which that Supplier Party can exchange files.

9.3 The DCC shall securely exchange only those files which are relevant to a Supplier Party with that Supplier Party through DCC's Microsoft SharePoint.

10 SMETS1 Migration Schema

10.1 This Clause 10 incorporates the SMETS1 Migration Schema, with which the contents of files created pursuant to this TMAD shall comply, if they are to be valid and authentic. For each file type, the contents shall be a single instance of the XML structure specified in Table 10.2. Each such XML structure shall be populated with information, within each element, as required by Table 10.1 in the format specified by the SMETS1 Migration Schema embedded below.

SMETS1 Migration Schema v1.2_MOC_F

XML Element	Information
CHFDetail	The information required in relation the SMETS1 CHF which forms part of this SMETS1 Installation and which is required in order to carry out the checks and processing in this TMAD. As per the SMETS1 Migration Schema, this shall not contain any of: • CriticalNetworkOperatorCertificateID • NonCriticalNetworkOperatorCertificateID • CriticalSupplierCertificateID • NonCriticalSupplierCertificateID
GPFDetail	The information required in relation the SMETS1 GPF which forms part of this SMETS1 Installation and which is required in order to carry out the checks and processing in this TMAD. As per the SMETS1 Migration Schema, this shall contain one and only one of each of: • CriticalNetworkOperatorCertificateID • NonCriticalNetworkOperatorCertificateID • CriticalSupplierCertificateID • NonCriticalSupplierCertificateID Where the SMETS1Installation does not contain a GSME, the values in the above four elements shall be the Null Certificate ID.
ESMEDetail	The information required in relation the SMETS1 ESME which forms part of this SMETS1 Installation and which is required in order to carry out the checks and processing in this TMAD. As per the SMETS1 Migration Schema, this shall contain one and only one of each of: • CriticalNetworkOperatorCertificateID • NonCriticalNetworkOperatorCertificateID • CriticalSupplierCertificateID • NonCriticalSupplierCertificateID

XML Element	Information
GSMEDetail	The information required in relation the SMETS1 GSME which forms part of this SMETS1 Installation and which is required in order to carry out the checks and processing in this TMAD. As per the SMETS1 Migration Schema, this shall contain one and only one of each of: • CriticalSupplierCertificateID • NonCriticalSupplierCertificateID As per the SMETS1 Migration Schema, this shall contain not contain: • CriticalNetworkOperatorCertificateID • NonCriticalNetworkOperatorCertificateID
IHDDetail	The information required in relation the SMETS1 IHD which forms part of this SMETS1 Installation and which is required in order to carry out the checks and processing in this TMAD. As per the SMETS1 Migration Schema, this shall not contain any of: • CriticalNetworkOperatorCertificateID • NonCriticalNetworkOperatorCertificateID • CriticalSupplierCertificateID • NonCriticalSupplierCertificateID
PPMIDDetail	The information required in relation the SMETS1 PPMID which forms part of this SMETS1 Installation and which is required in order to carry out the checks and processing in this TMAD. As per the SMETS1 Migration Schema, this shall not contain any of: • CriticalNetworkOperatorCertificateID • NonCriticalNetworkOperatorCertificateID • CriticalSupplierCertificateID • NonCriticalSupplierCertificateID
CADDetail	The information required in relation the SMETS1 CAD which forms part of this SMETS1 Installation and which is required in order to carry out the checks and processing in this TMAD. As per the SMETS1 Migration Schema, this shall not contain any of: • CriticalNetworkOperatorCertificateID • NonCriticalNetworkOperatorCertificateID • CriticalSupplierCertificateID • NonCriticalSupplierCertificateID
DeviceDetail	For the Device to which this element relates, the combination of FirmwareVersion, DeviceModel, DeviceManufacturer (so equating to Device Model) and DeviceType (equating to Device Type)
FirmwareVersion	For the Device to which this element relates, the value required by DUIS in the FirmwareVersion element
DeviceType	For the Device to which this element relates, the value required by DUIS in the DeviceType element
DeviceModel	For the Device to which this element relates, the value required by DUIS in the DeviceModel element
DeviceManufacturer	For the Device to which this element relates, the value required by DUIS in the DeviceManufacturer element
DeviceID	The Device ID of the Device to which this element relates
RequestingPartyID	The DCC ID of the relevant Requesting Party which shall have the same value as Entity Identifier in the Organisation Certificate identified in the X509IssuerSerial element in the file.
S1SPID	The DCC ID of the relevant S1SP which shall have the same value as Entity Identifier in the Organisation Certificate identified in the X509IssuerSerial element in the file.

XML Element	Information
CommissioningPartyID	The DCC ID of the Commissioning Party which shall have the same value as Entity Identifier in the Organisation Certificate identified in the X509IssuerSerial element in the file.
GroupID	The GroupID for the set of SMETS1 Installations detailed in this file.
CriticalNetworkOperatorCertificateID	Where no Network Party is identified, the Null Certificate ID; otherwise a Certificate ID identifying a Certificate which contains the Critical Network Operator ID
NonCriticalNetworkOperatorCertificateID:	Where no Network Party is identified, the Null Certificate ID; otherwise a Certificate ID identifying a Certificate which contains the Non-Critical Network Operator ID
CriticalSupplierCertificateID:	Where no Supplier Party is identified, the Null Certificate ID; otherwise a Certificate ID identifying a Certificate which contains the Critical Supplier ID
NonCriticalSupplierCertificateID:	Where no Supplier Party is identified, the Null Certificate ID; otherwise a Certificate ID identifying a Certificate which contains the Non-Critical Supplier ID
SMETS1Installation	The information required in relation to a SMETS1 Installation in order to carry out the checks and processing in this TMAD.
X509IssuerSerial	In relation to the Signature element, the Certificate ID, which is composed of the X509SerialNumber and X509IssuerName, of the Organisation Certificate that can be used to verify the SignatureValue. In other uses, contains the Certificate ID of the relevant Certificate.
X509SerialNumber	Contains the serialNumber (with its Organisation Certificate Policy meaning) of the relevant Certificate
X509IssuerName	Contains the issuerName (with its Organisation Certificate Policy meaning) of the relevant Certificate
MCFCounter	The current value of the Requesting Party's Migration Common File Counter.
MGFCounter	The current value of the Requesting Party's Migration Group File Counter
MEFCounter	The current value of the Requesting Party's Migration Group Encrypted File Counter
MVFCounter	The current value of the DCC's Migration Common Validation File Counter
SCFCounter	The current value of the S1SP's S1SP Commissioning File Counter
COFCounter	The current value of the Commissioning Party's Commissioning Outcome File Counter
FailedCheck	An element detailing the outcome of a failed check undertaken pursuant to this TMAD
FailedStepNumber	An element detailing which check failed
SupportingData	Additional data associated with a failed check
CHFIdentifier	The DeviceID in the CHFDetail
CertificateID	For the Supporting Data in the Table 5.10
CertificatePair	For the Supporting Data in the Table 5.10
EncryptedS1SPGroupInformation	As required by Table 11.2.1
DecryptedS1SPGroupInformation	As required by Table 11.2.1
EncryptedMasterKey	Either: • A structure containing one EncryptedKey and a list of one of more DeviceIDs identifying which of the ESME, GPF and CHF the corresponding EncryptedKey is the Master Key (with its DLMS COSEM meaning) for; or • A structure containing one EncryptedKey and the DeviceID of the PPMID where the corresponding EncryptedKey is the Master Key (with its DLMS COSEM meaning) for the PPMID.

<table>
<tr><th>XML Element</th><th>Information</th></tr>
<tr><td>Signature</td><td>As required by Clause 5.5, each of the objects in Table 5.5 shall incorporate a Digital Signature (XMLDSig) generated using the Elliptic Curve Digital Signature Algorithm (ECDSA), and a Private Key for which the associated Public Key is included in an Organisation Certificate with the Remote Party Role Code as in the table in Annex A to Section L.

The parameters and algorithms used shall be

<table>
<tr><th>Parameter/Algorithm</th><th>Value</th></tr>
<tr><td>Reference URI</td><td>“”</td></tr>
<tr><td>Transform Algorithm</td><td>http://www.w3.org/2000/09/xmldsig#enveloped-signature</td></tr>
<tr><td>CanonicalizationMethod Algorithm</td><td>http://www.w3.org/2001/10/xml-exc-c14n#</td></tr>
<tr><td>SignatureMethod Algorithm</td><td>http://www.w3.org/2001/04/xmldsig-more#ecdsa-sha256</td></tr>
<tr><td>DigestMethod Algorithm</td><td>http://www.w3.org/2001/04/xmlenc#sha256</td></tr>
</table></td></tr>
<tr><td>KeyInfo</td><td>Shall contain an X509IssuerSerial element (in a single X509Data element) which shall identify the Organisation Certificate that can be used to Check Cryptographic Protection</td></tr>
<tr><td>ToBeCommissionedByDCC</td><td>As required by Clause 5.10</td></tr>
<tr><td>PrepayFlag</td><td>As required by Appendix A of this TMAD.</td></tr>
<tr><td>ESMEVariant</td><td>For the Device to which this element relates, the value required by DUIS in the ESMEVariant</td></tr>
<tr><td>ImportMPAN</td><td>For the Device to which this element relates, the value required by DUIS in the ImportMPxN</td></tr>
<tr><td>MPRN</td><td>For the Device to which this element relates, the value required by DUIS in the ImportMPxN</td></tr>
<tr><td>ReportingPartyID</td><td>The DCC ID of the part of the DCC creating the file, which shall have the same value as Entity Identifier in the Organisation Certificate identified in the X509IssuerSerial element in the file.</td></tr>
<tr><td>IMSI</td><td>The international mobile subscriber identity of the SIM Card used in Comms Hub</td></tr>
<tr><td>IPAddr</td><td>The static IP address associated with the SIM identified by IMSI</td></tr>
<tr><td>DNSServer</td><td>The DNS server IP address configured on the SIM identified by IMSI</td></tr>
<tr><td>PingServer</td><td>The ping server IP address configured on the SIM identified by IMSI</td></tr>
<tr><td>PreviousAPN</td><td>The access point name configured for the SIM identified by IMSI</td></tr>
<tr><td>SerialNumbers</td><td>Each string within SerialNumbers is the serial number of the relevant Device</td></tr>
</table>

Table 10.1

10.2 Each file shall be named according to the following requirements:

FileType_RequesterID_MCFCounter_AdditionalID.xml

where:

- MCFCounter have the values as per the content of the files (so in all cases correspond to the Migration Common File which triggered the processing for the SMETS1 Installation(s) detailed in the file); and

- FileType, RequesterID and AdditionalID have the values required by Table 10.2.

Type of file	FileType value	RequesterID value	AdditionalID value	XML structure within file
Commissioning Outcome File	'COF'	Supplier Signifier value from S1SP Commissioning File filename and ReportingPartyID value concatenated using an "_" (underscore).	COFCounter value from the file	CommissioningOutcomes
Migration Common File	'MCF'	RequestingPartyID value from the file when named by the Requesting Party. When the DCC intends to send to the Registered Supplier over the SMETS1 Migration Interface, RequesterID shall be the Supplier Signifier followed by an "_" (underscore) followed by RequestingPartyID value from the file.	Zero	MigrationCommon
Migration Group File	'MGF'	RequestingPartyID value from the file	MGFCounter value from the file	MigrationGroup
Migration Group Encrypted File	'MEF'	RequestingPartyID value from the file	MEFCounter value from the file	MigrationGroupEncrypted
Migration Common Validation File	'MVF'	ReportingPartyID value from the file	MVFCounter value from the file	MigrationValidation
S1SP Commissioning File	'SCF'	Supplier Signifier and ReportingPartyID value from the file concatenated using an "_" (underscore).	SCFCounter value from the file	S1SPOutcomes

Table 10.2

11 File Content Encryption and Decryption

11.1 A Requesting Party shall only have access to any populated EncryptedS1SPGroupInformation and MasterKeyInformation, where required for the specified GroupID, provided by the relevant SMETS1 SMSO, and shall not have access to either the Plaintext or symmetric keys which were used as input to the population of such elements.

11.2 When a SMETS1 SMSO generates a 128 bit symmetric key for use in relation to this Clause 11, the DCC shall ensure that the SMETS1 SMSO;

(a) generates a new such key for each EncryptedS1SPGroupInformation it creates;

(b) generates each such key using random numbers such as to make it computationally infeasible to regenerate the key even with knowledge of when and by means of what equipment it was

generated; and

(c) populates each EncryptedS1SPGroupInformation in line with the requirement of Table 11.2.1 and Table 11.2.2

Terms in Table 11.2.1 shall have the meanings in NIST Special Publication 800-38D November, 2007 (https://csrc.nist.gov/publications/detail/sp/800-38d/final).

Terms in Table 11.2.2 and Table 11.3 shall have the meanings in IETF RFC 8017 (https://tools.ietf.org/html/rfc8017).

Attribute	**Values**
Plaintext	A string containing fully populated DecryptedS1SPGroupInformation
Algorithm	AES-GCM-128
Key	The number generated pursuant to Clause 11.2
Initialization Vector	0x000000000000000000000000
Additional Authenticated Data	Empty string
ProtectedData within the EncryptedS1SPGroupInformation	Base64 encoded Ciphertext
AuthenticationTag within the EncryptedS1SPGroupInformation	Base64 encoded 128 bit Authentication Tag

Table 11.2.1

Attribute	**Values**
Algorithm	RSAES-OAEP
Label hash	SHA-256
Mask Generation Function	MGF1 with SHA-1 hash

Recipient's RSA public key	As pursuant to Clause 5.1(a)
Message to be encrypted	The number generated pursuant to Clause 11.2
Label	Empty string
WrappedTransportKey within the EncryptedS1SPGroupInformation	Base64 encoded Ciphertext

Table 11.2.2

11.3 The DCC shall ensure that each SMETS1 SMSO shall populate EncryptedMasterKey element according to Table 11.3

Attribute	**Values**
Algorithm	RSAES-OAEP
Label hash	SHA-256
Mask Generation Function	MGF1 with SHA-256 hash
Recipient's RSA public key	As pursuant to Clause 5.1(a)
Message to be encrypted	Master Key (with its DLMS COSEM meaning) for the Device(s) identified by DeviceID(s) within EncryptedMasterKey
Label	Empty string
EncryptedKey within the EncryptedMasterKey	Base64 encoded Ciphertext
DeviceID(s) within EncryptedMasterKey	The DeviceID of the Devices for which EncryptedMasterKey contains the Master Key with its DLMS COSEM meaning

Table 11.3

11.3B For GroupID = “DA”, the DCC shall ensure that each SMETS1 SMSO shall populate any required EncryptedSUAKey element according to Table 11.3B

Attribute	Values
Algorithm	RSAES-OAEP
Hash	SHA-256
Mask Generation Function	MGF1
Recipient's RSA public key	As pursuant to Clause 5.1(a)
Message to be encrypted	The symmetric key required by the DCO to begin controllinginstructions for the Device
Label	Empty string
EncryptedSUAKey within the SUAKeyDetails	Base64 encoded Ciphertext
DeviceType within SUAKeyDetails	The Device Type of the Device being “ESME” or “GSME”.
PublicKey within SUAKeyDetails	The Base64 encoded uncompressed form of the Elliptic Curve P-256 Public Key, corresponding to the Private Key used for signing ephemeral keys during key establishment with DCO. This is the concatenation 0x04 || X || Y, where len(X)=len(Y)=32 bytes for a 256 bits curve.
SerialNumber within SUAKeyDetails	The Device serial number (according to information held by the relevant SMETS1 SMSO) for the Device.

Table 11.3B

11.4 ensure that each SMETS1 SMSO shall populate any WrappedPrepaymentKey element where it is required for the specified GroupID according to Table 11.4

Terms in Table 11.4 shall have the meanings in IETF RFC 3394 (https://tools.ietf.org/html/rfc3394).

Attribute	Values
Plaintext	The PrepaymentKey within ManagementAssociation for the Device

Algorithm	AES Key Wrap
Key	Master Key (with its DLMS COSEM meaning) for the Device
WrappedPrepaymentKey within the ManagementAssociation	Base64 encoded Ciphertext

Table 11.4

11.5 The DCC shall ensure that each SMETS1 SMSO shall, in populating any required EncryptedS1SPGroupInformation and MasterKeyInformation elements to provide them to the Requesting Party, not decrease the security of the Secret Key Material used as input to the formation of the corresponding Plaintext.

11.6 Where the SMETS1 SMSO and Requesting Party exchange information pursuant to this TMAD, the DCC shall ensure that they shall do so in a way which ensures the information cannot be read by any other entity.

12 Requirements specific to GroupID = "AA"

12.1 This Clause 12 specifies the requirements which are specific to processing in relation to SMETS1Installations where GroupID = "AA".

Pre-enrolment Configuration Requirements

12.2 NOT USED

Migration Group Encrypted File

12.3 A Migration Group Encrypted File is required for this GroupID.

S1SP Required File Set

12.4 The S1SP Required File Set consists of one Migration Common File, one Migration Common Validation File, one Migration Group File and one Migration Group Encrypted File, all with the same Migration Header, and so the same GroupID.

DCO Required File Set

12.5 The DCO Required File Set consists of one Migration Common File, one Migration Common

Validation File and one Migration Group Encrypted File, all with the same Migration Header, and so the same GroupID.

S1SP Migration Group File data validation

12.6 The checks at Table 12.6 shall be the 'S1SP Migration Group File data validation' for this GroupID.

Step number	Check and processing
	Should the following check fail, checking in relation to that SMETS1 Installation shall cease

12.6.1	Confirm the following are present and populated validly within the entry with the CHFIdentifier for this SMETS1 Installation:
	• for the CHFDetails:
	  • IMSI
	  • PreviousAPN
	  • SerialNumbers

Table 12.6

DCO Migration Group Encrypted File data validation

12.7 The checks at Table 12.7 shall be the 'DCO Migration Group Encrypted File data validation' for this GroupID.

Step number	Check and processing
	Should any of the following checks fail, checking in relation to that SMETS1 Installation shall cease
12.7.1	Confirm the following are present and populated validly for the entry with the CHFIdentifier for this SMETS1 Installation: • an EncryptedKeyGPF, and EncryptedKey element within the EncryptedMasterKeyand an EncryptedKey element within the EncryptedMasterKey which contains the DeviceID of the ESME

Table 12.7

S1SP Migration Group Encrypted File data validation

12.8 The checks at Table 12.8 shall be the 'S1SP Migration Group Encrypted File data validation' for this GroupID.

Step number	Check and processing
	Should any of the following checks fail, checking in relation to that SMETS1 Installation shall cease

12.8.1	Confirm the following are present and populated validly within the DecryptedS1SPGroupInformation for the entry with the CHFIdentifier for this SMETS1 Installation:
	• for each of the DataCollectionAssociation, ExtendedDataCollectionAssociation, ManagementAssociation and FirmwareAssociation within each of the CHFDetails, GPFDetails and ESMEDetails:
	  • AuthenticationKey
	  • EncryptionKey
	• for the ESMEDetails:
	  • PrepaymentKey

12.8.2	If there is a GSMEIdentifier for this SMETS1 Installation in the Migration Common File, confirm the following are present and populated validly within the DecryptedS1SPGroupInformation for the GSMEDetails within the entry with the CHFIdentifier for this SMETS1 Installation: • PrepaymentKey

Table 12.8

S1SP / DCO Commissioning of SMETS1 Installation

12.9 The checks at Table 12.9 shall be the 'S1SP / DCO Commissioning of SMETS1 Installation' for this GroupID.

StepNumber	Check and processing	Critical?	SupportingData
	Should any of the following checks which are marked 'Critical' fail, checking in relation to that SMETS1 Installation shall cease		
12.9.1.X	The checks and processing required for 'Installing a SMETS1 Electricity Meter' for this GroupID, as specified in 17.12 of this TMAD, shall be undertaken. For clarity, this includes retrieval of the CHF Whitelist. The information returned shall be that used in subsequent steps.	Yes	The error code for any failure that occurs, as defined in 17.12 of this TMAD.
12.9.2.X	Where a GSMEDetail element is present, the checks and processing required for 'Installing a SMETS1 GSME' for this GroupID, as specified in 17.12 of this TMAD, shall be undertaken.	Yes	The error code for any failure that occurs, as defined in 17.12 of this TMAD.
12.9.1.X	The checks and processing required for 'Securing a SMETS1 ESME' for this GroupID, as specified in 17.12 of this TMAD, shall be undertaken.	Yes	The error code for any failure that occurs, as defined in 17.12 of this TMAD.
12.9.3.X	Where a PPMIDDetail element is present, the checks and processing required for 'Installing a SMETS1 PPMID' for this GroupID, as specified in 17.12 of this TMAD, shall be undertaken.	Yes	The error code for any failure that occurs, as defined in 17.12 of this TMAD.
12.9.4	Where the CHF is of a Device Model which requires the ESME Device Identifier to be in the CHF Whitelist, check that the ESME Device Identifier, included in the Migration Common File for this SMETS1 Installation, is included in the CHF Whitelist retrieved at StepNumber 1.	Yes	
12.9.5	Where a GSME Device Identifier is included in the Migration Common File for this SMETS1 Installation, check that that GSME Device Identifier is included in the CHF Whitelist retrieved at StepNumber 12.9.1.	Yes	
12.9.6	Where a PPMID Device Identifier is included in the Migration Common File for this SMETS1 Installation, check that that PPMID Device Identifier is included in the CHF Whitelist retrieved at StepNumber 12.9.1.	Yes	
12.9.7.X	For the CHF identified in the Migration Common File for this SMETS1 Installation, undertake the 17.12 of this TMAD required 'Commission Device (CHF)' processing for this GroupID and confirm it is successful. For clarity, the DCC shall only return a response indicating success if the CHF Smart Metering Inventory Status is successfully set to 'Commissioned'.	Yes	The error code for any failure that occurs, as defined in 17.12 of this TMAD.

Table 12.9

Installation Rollback

12.10 The processing at Table 12.10 shall be the 'Installation Rollback' for this GroupID**.**

Step number	Check and processing
12.10.1	The DCO shall delete any keys and related information it has stored pursuant to Clause 5.27 in relation to this SMETS1 Installation. The DCO shall either successfully delete all such keys and information or raise an Incident if it cannot.
12.10.2	The S1SP shall delete any keys and information it has stored pursuant to Clause 5.27 in relation to this SMETS1 Installation. The S1SP shall either successfully delete all such keys and information or raise an Incident if it cannot.
12.10.3	The S1SP shall take reasonable steps to restore WAN communication between SMETS1 Installation and the relevant SMETS1 SMSO.

Table 12.10

CHF Whitelist

12.11 The CHF Whitelist shall, for this GroupID, include, for each IEEE address either (1) the UTC date-time at which the CHF last communicated with the identified Device or (2) an indication that the CHF has never communicated with the identified Device.

12.12 The CHF Whitelist shall never include Device IDs for a CHF or a GPF and shall always include

the Device ID for an ESME.

Post Migration Configuration

12.13 NOT USED.

Migration Group File

12.14 A Migration Group File is required for this Group ID.

Additional File Structure Validation

12.15 A Migration Group Encrypted File is required for this Group ID, and each such file must include EncryptedS1SPGroupInformation and EncryptedMasterKey, and must not include any SUAKeyDetails.

Migration Common File Device Selection Requirements

12.16 NOT USED.

13 Requirements specific to GroupID = "BA"

13.1 This Clause 13 specifies the requirements which are specific to processing in relation to SMETS1Installations where GroupID ="BA".

Pre-enrolment Configuration Requirements

13.2 NOT USED.

13.3 The DCC shall ensure that each SMETS1 SMSO shall populate the PrepaymentKey within DecryptedS1SPGroupInformation in Migration Group File with the key used for UTRN generation with;

(a) Where it currently holds such a value, that value; or

(b) Where it does not currently hold such a value, a value it generates. It shall generate such values using random numbers such as to make it computationally infeasible to regenerate the values even with knowledge of when and by means of what equipment they were generated.

13.4 The WrappedPrepaymentKey is required for this GroupID and so shall be populated by the

SMETS1 SMSO pursuant to Clause 11.4.

Migration Group Encrypted File

13.5 A Migration Group Encrypted File is required for this GroupID.

S1SP Required File Set

13.6 The S1SP Required File Set consists of one Migration Common File, one Migration Common Validation File, one Migration Group File and one Migration Group Encrypted File, all with the same Migration Header, and so the same GroupID.

DCO Required File Set

13.7 The DCO Required File Set consists of one Migration Common File, one Migration Common Validation File and one Migration Group Encrypted File, all with the same Migration Header, and so the same GroupID.

S1SP Migration Group File data validation

13.8 Clause 12.6 shall apply.

DCO Migration Group Encrypted File data validation

13.9 The checks at Table 13.9 shall be the 'DCO Migration Group Encrypted File data validation' for this GroupID.

Step number	Check and processing
	Should any of the following checks fail, checking in relation to that SMETS1 Installation shall cease
13.9.1	Confirm the following are present and populated validly for the entry with the CHFIdentifier for this SMETS1 Installation: • an EncryptedKey element within the EncryptedMasterKey which contains the DeviceID for each of the CHF, the GPF and the ESME

Table 13.9

S1SP Migration Group Encrypted File data validation

13.10 The checks at Table 13.10 shall be the 'S1SP Migration Group Encrypted File data validation' for this GroupID.

Step number	Check and processing
	Should any of the following checks fail, checking in relation to that SMETS1 Installation shall cease

13.10.1	Confirm the following are present and populated validly within the DecryptedS1SPGroupInformation for the entry with the CHFIdentifier for this SMETS1 Installation:
	• for each of the DataCollectionAssociation, ExtendedDataCollectionAssociation, ManagementAssociation and FirmwareAssociation within each of the CHFDetails, GPFDetails and ESMEDetails:
	  • AuthenticationKey
	  • EncryptionKey

Table 13.10

S1SP / DCO Commissioning of SMETS1 Installation

13.11 Clause 12.9 shall apply.

Installation Rollback

13.12 Clause 12.10 shall apply.

CHF Whitelist

13.13 The CHF Whitelist shall, for this GroupIDs, include, for each IEEE address, either (1) the UTC date-time at which the CHF last communicated with the identified Device or (2) an indication that the CHF has never communicated with the identified Device.

13.14 The CHF Whitelist shall never include Device IDs for a CHF, a GPF or an ESME and shall only include the Device ID for a GSME where that GSME communicates with the GPF using a ZigBee network.

Post Migration Configuration

13.15 NOT USED

Additional File Structure Validation

13.16 Clause 12.15 shall apply.

Migration Common File Device Selection Requirements

13.17 NOT USED.

14 Requirements specific to GroupID = “CA” or “CB”

14.1 This Section 14 specifies the requirements which are specific to processing in relation to SMETS1Installations where GroupID =”CA” or “CB”.

Pre-enrolment Configuration Requirements

14.2 The DCC shall ensure that each SMETS1 SMSO shall take reasonable steps to configure WAN

communication between SMETS1 Installation and the relevant S1SP.

14.3 To enable Clause 14.2 for GroupID = "CB", the DCC shall ensure that the communication services provider takes all reasonable steps to carry out any precursor steps that are necessary to allow the SMETS1 SMSO to configure the WAN in accordance with Clause 14.2 and provide any relevant information to the SMETS1 SMSO.

Migration Group Encrypted File

14.4 A Migration Group Encrypted File is required for these GroupIDs.

S1SP Required File Set

14.5 The S1SP Required File Set consists of one Migration Common File, one Migration Common Validation File, one Migration Group File and one Migration Group Encrypted File, all with the same Migration Header, and so the same GroupID.

DCO Required File Set

14.6 The DCO Required File Set consists of one Migration Common File, one Migration Common Validation File and one Migration Group Encrypted File, all with the same Migration Header, and so the same GroupID.

S1SP Migration Group File data validation

14.7 The checks at Table 14.7 shall be the 'S1SP Migration Group File data validation' for these GroupIDs.

Step number	Check and processing
	Should any of the following checks fail, checking in relation to that SMETS1 Installation shall cease

14.7.1	Confirm the following are present and populated validly within the entry with the CHFIdentifier for this SMETS1 Installation:
	• for the CHFDetails:
	  • IMSI
	  • IPAddr
	  • PreviousAPN
	  • SerialNumbers

Table 14.7

DCO Migration Group Encrypted File data validation

14.8 The checks at Table 14.8 shall be the 'DCO Migration Group Encrypted File data validation' for these GroupIDs.

Step number	Check and processing
	Should any of the following checks fail, checking in relation to that SMETS1 Installation shall cease

Step number	Check and processing
14.8.1	Confirm the following are present and populated validly for the entry with the CHFIdentifier for this SMETS1 Installation: • an EncryptedKey element within the EncryptedMasterKey which contains the DeviceID of the CHF, an EncryptedKey element within the EncryptedMasterKey which contains the DeviceID of the GPF and an EncryptedMasterKey element which contains the DeviceID of the ESME

Table 14.8

S1SP Migration Group Encrypted File data validation

14.9 The checks at Table 14.9 shall be the 'S1SP Migration Group Encrypted File data validation' for this GroupID.

Step number	Check and processing
	Should any of the following checks fail, checking in relation to that SMETS1 Installation shall cease

14.9.1	Confirm the following are present and populated validly within the DecryptedS1SPGroupInformation for the entry with the CHFIdentifier for this SMETS1 Installation:
	• for each of the DataCollectionAssociation, ExtendedDataCollectionAssociation, ManagementAssociation and FirmwareAssociation within each of the CHFDetails, GPFDetails and ESMEDetails:
	  • AuthenticationKey
	  • EncryptionKey

Table 14.9

S1SP / DCO Commissioning of SMETS1 Installation

14.10 Clause 12.9 shall apply.

Installation Rollback

14.11 Clause 12.10 shall apply.

CHF Whitelist

14.12 The CHF Whitelist shall, for this GroupID, include, for each IEEE address either (1) the UTC date-time at which the CHF last communicated with the identified Device or (2) an indication that the CHF has never communicated with the identified Device.

14.13 The CHF Whitelist shall never include Device IDs for a CHF, a GPF or an ESME and shall only include the Device ID for a GSME where that GSME communicates with the GPF using a ZigBee network.

Post Migration Configuration

14.14 For GroupID = "CB", the DCC shall ensure that the communications services provider takes all reasonable steps to ensure that the SMETS1 SMSO can no longer communicate with the Commissioned SMETS1 Devices or any associated communications service provider systems.

Migration Group File

14.15 A Migration Group File is required for this Group ID.

Additional File Structure Validation

14.16 Clause 12.15 shall apply.

Migration Common File Device Selection Requirements

14.17 NOT USED.

15 Requirements specific to GroupID = “EA”, “EB” and “EC”

[Placeholder for FOC TMAD content]

16 Requirements specific to GroupID = "DA"

16.1 This Clause 16 specifies the requirements which are specific to processing in relation to SMETS1 Installations where GroupID = "DA".

Pre-enrolment Configuration Requirements

16.2 NOT USED

Migration Group Encrypted File

16.3 A Migration Group Encrypted File is required for this GroupID.

S1SP Required File Set

16.4 The S1SP Required File Set consists of one Migration Common File, one Migration Common Validation File, and one Migration Group Encrypted File, all with the same Migration Header, and so the same GroupID.

DCO Required File Set

16.5 The DCO Required File Set consists of one Migration Common File, one Migration Common Validation File and one Migration Group Encrypted File, all with the same Migration Header, and so the same GroupID.

S1SP Migration Group File data validation

16.6 NONE REQUIRED.

DCO Migration Group Encrypted File data validation

16.7 The checks at Table 16.7 shall be the 'DCO Migration Group Encrypted File data validation' for this GroupID.

Step	Check and processing
	Should any of the following checks fail, checking in relation to that SMETS1 Installation shall cease
16.7.1	For each SMETS1Installation, confirm there are no EncryptedMasterKey elements.
16.7.2	For each SMETS1Installation, confirm there is one and only one EncryptedSUAKey (referring to a SUA Symmetric Key) element with DeviceType of "ESME".
16.7.3	If according to the "Migration Common File" there is a "GSME" in this SMETS1Installation, confirm there is one and only one other EncryptedSUAKey (referring to a SUA Symmetric Key) element which has a DeviceType of "GSME".
16.7.4	If according to the "Migration Common File" there is no "GSME" in this SMETS1Installation, confirm there is no other EncryptedSUAKey (SUA Symmetric Keys) element.
16.7.5	For each SMETS1Installation, confirm that there is no empty child element within any SUAKeyDetails element.

Table 16.7

S1SP Migration Group Encrypted File data validation

16.8 NONE REQUIRED.

S1SP / DCO Commissioning of SMETS1 Installation

16.9 The steps at Table 16.9 may be carried out by the DCC up to 7 days in advance of the other steps in Clause 5.27 for the SMETS1 Installation in question.

SupportingData

StepNumber	Check and processing	Critical?	
	Should any of the following checks which are marked 'Critical' fail, checking in relation to that SMETS1 Installation shall cease		

SupportingData			
16.9.1.x	The checks and processing required for 'Installing a SMETS1 Electricity Meter' for this GroupID, as specified in Appendix C of this TMAD, shall be undertaken. For clarity, this includes retrieval of the CHF Whitelist. The information returned shall be that used in subsequent steps.	Yes	The error code for any failure that occurs, as defined in Appendix C of this TMAD.
16.9.2.x	Where a GSMEDetail element is present, the checks and processing required for 'Installing a SMETS1 GSME' for this GroupID, as specified in Appendix CAppendix B of this TMAD, shall be undertaken.	Yes	The error code for any failure that occurs, as defined in Appendix C of this TMAD.
16.9.3	Where a PPMIDDetail element is present, the checks and processing required for 'Installing a SMETS1 PPMID' for this GroupID, as specified in Appendix C of this TMAD, shall be undertaken.	Yes	The error code for any failure that occurs, as defined in Appendix C of this TMAD.
16.9.4	Where a PPMID Device Identifier is included in the Migration Common File for this SMETS1 Installation, check that that PPMID Device Identifier is included in the CHF Whitelist retrieved at StepNumber 16.9.1.	Yes	

Table 16.9

16.10 The steps at Table 16.10 shall not be carried out in advance of the other steps in Clause 5.27 for the SMETS1 Installation in question.

StepNumber	Check and processing	Critical?	SupportingData
	Should any of the following checks which are marked 'Critical' fail, checking in relation to that SMETS1 Installation shall cease		
16.10.1.X	Where a GSMEDetail element is present, the checks and processing required for 'Securing a SMETS1 GSME' for this GroupID, as specified in Appendix C of this TMAD, shall be undertaken.	Yes	The error code for any failure that occurs, as defined in 17.12 of this TMAD.
16.10.2.X	The checks and processing required for 'Securing a SMETS1 ESME' for this GroupID, as specified in Appendix B of this TMAD, shall be undertaken.	Yes	The error code for any failure that occurs, as defined in 17.12 of this TMAD.
16.10.3.X	For the CHF identified in the Migration Common File for this SMETS1 Installation, undertake the checks and processing required for 'Commission Device (CHF)' for this GroupID, as specified in Appendix C of this TMAD, and confirm it is successful. For clarity, the DCC shall only return a response indicating success if the CHF Smart Metering Inventory Status is successfully set to 'Commissioned'.	Yes	The error code for any failure that occurs, as defined in Appendix C of this TMAD.

Table 16.10

Installation Rollback

16.11 The processing at Table 16.11 shall be the 'Installation Rollback' for this GroupID.

Step	Check and processing
16.11.1	If GSME is present, the S1SP shall revert control of the SMETS1 Installation to the relevant SMETS1 SMSO where any of the steps in "Securing a SMETS1 GSME" fails for this GroupID . The S1SP shall not revert control of the SMETS1 Installation to the relevant SMETS1 SMSO if any of the steps in "Securing a SMETS1 ESME" fails for this GroupID.

Table 16.11

CHF Whitelist

16.12 The CHF Whitelist shall, for this GroupID, include, for each IEEE address either (1) the UTC date-time at which the CHF last communicated with the identified Device or (2) an indication that the CHF has never communicated with the identified Device.

16.13 The CHF Whitelist shall never include Device IDs for a CHF, a GPF or an ESME and shall only include the Device ID for a GSME where that GSME communicates with the GPF.

Post Migration Configuration

16.14 NOT USED.

Migration Group File

16.15 A Migration Group File is not required for this GroupID.

Additional File Structure Validation

16.16 A Migration Group Encrypted File is required for this GroupID, and each such file must not include any EncryptedS1SPGroupInformation or any EncryptedMasterKey, and must include SUAKeyDetails.

Migration Common File Device Selection Requirements

16.17 Where there is more than one SMETS1 PPMID, SMETS1 IHD or SMETS1 CAD in a SMETS1 Installation that solely comprises Dormant meters, the DCC shall include only one of each Device Type in the Migration Common File, being the one that most recently joined the HAN.

17 SMETS1 Device Security Testing

17.1 The DCC shall carry out SMETS1 Device Security Testing in accordance with the requirements of this Clause 17 for the purpose of identifying security risks to the DCC Total System.

17.2 Each Supplier Party hereby acknowledges that in preparing and conducting SMETS1 Device Security Testing under this Clause 17, the DCC does not warrant or represent that SMETS1 Device Models or combinations of SMETS1 Device Models operate or do not operate in a particular way when comprising part of an Enrolled SMETS1 Smart Metering System.

17.3 No later than 5 Working Days following this Clause 17.3 coming into effect, the DCC shall submit the SMETS1 Device Security Testing Scope and Timetable Document to the Security Sub-Committee (and such submission may take place prior to this this Clause 17.3 coming into effect). The SMETS1 Device Security Testing Scope and Timetable Document shall set out:

(a) the SMETS1 Device Models (and, where relevant, the combinations of SMETS1 Device Models) that are to be the subject of SMETS1 Device Security Testing which shall be those SMETS1 Device Models proposed to the Security Sub-Committee for the purposes of SMETS1 Device Security Testing by the DCC on 14 May 2020;

(b) the nature of the tests (including negative tests) that are to be carried out as part of SMETS1 Device Security Testing, which shall be those tests that were agreed by the Security Sub-Committee for the purposes of SMETS1 Device Security Testing on 8 January 2020; and

(c) the associated reasonable timetable in accordance with which the tests are to be carried out.

17.4 The DCC may seek variations to the SMETS1 Device Security Testing Scope and Timetable Document by submitting a revised draft SMETS1 Device Security Testing Scope and Timetable Document to the Security Sub-Committee for review, provided that the nature of the tests may not be modified so as to result in a material deviation from the implicit purposes of the tests referred to in Clause 17.3 (b):

(a) where the Security Sub-Committee and the DCC can reach an agreement, the relevant revised draft SMETS1 Device Security Testing Scope and

Timetable Document shall be updated by the DCC as necessary and deemed to be final; or

(b) where the Security Sub-Committee and the DCC cannot reach an agreement, the relevant revised draft SMETS1 Device Security Testing Scope and Timetable Document shall be referred by the DCC to the Secretary of State for determination (whose decision shall be final and binding for the purposes of this Code) and the relevant revised draft SMETS1 Device Security Testing Scope and Timetable Document shall be updated by the DCC as necessary and deemed to be final.

17.5 The DCC shall take reasonable steps to complete the tests set out in the SMETS1 Device Security Testing Scope and Timetable Document in accordance with the timetable set out therein.

17.6 Revisions to the SMETS1 Device Security Testing Scope and Timetable Document finalised pursuant to Clause 17.4 may, from time to time be submitted by the DCC to the Security Sub-Committee in accordance with the provisions of Clause 17.4, and the provisions of Clauses 17.4 and 17.5 shall apply (again) to the revised version of the document.

17.7 The DCC shall take all reasonable steps to obtain a reasonable number of SMETS1 Devices for use in SMETS1 Device Security Testing and necessary consents.

17.8 In order that the DCC may perform SMETS1 Device Security Testing, any Supplier Party that is an Installing Supplier for any of the SMETS1 Device Models identified in the SMETS1 Device Security Testing Scope and Timetable Document shall take all reasonable steps to provide such support and assistance as the DCC may reasonably request including the provision of:

(a) such SMETS1 Devices; and

(b) firmware and firmware upgrades applicable to such SMETS1 Devices in an appropriate format to enable security testing consistent with the SMETS1 Device Security Testing Scope and Timetable Document.

17.9 Each Supplier Party providing SMETS1 Devices pursuant to Clause 17.8 is deemed to have provided consent, or procured consent, for the security

testing of such SMETS1 Devices consistent with the SMETS1 Device Security Testing Scope and Timetable Document.

17.10 SMETS1 Device Security Testing shall only be performed by the DCC using SMETS1 Devices which are installed in appropriate DCC appointed test laboratories.

17.11 Where the DCC reasonably considers that any SMETS1 Device Security Testing in relation to a relevant SMETS1 Device Model (or, where relevant, combinations of SMETS1 Device Models) is complete, the DCC shall, as soon as reasonably practicable, provide a report (being a SMETS1 Device Security Testing Completion Report) to the Security Sub-Committee setting out the results of such tests for review by the Security Sub-Committee. Following such review, the DCC shall update each SMETS1 Device Security Testing Completion Report to include any observations provided by the Security Sub-Committee and the DCC's responses to those observations and that SMETS1 Device Security Testing Completion Report shall be deemed to be final.

17.12 The DCC shall promptly provide each final SMETS1 Device Security Testing Completion Report to the Security Sub-Committee (and copied to the Secretary of State).

Appendix A **Device installation – For GroupIDs AA, BA, CA and CB**

A1 The Application Association labels:

(a) Public

(b) Data Collection

(c) Extended Data Collection

(d) Management

(e) Firmware

shall be the names allocated by the manufacturers of Devices in this group to the Application Associations accessible to the DCC.

Installing a SMETS1 Electricity Meter

A2 The checks and processing at Table A2 shall be that required of the S1SP and DCO for 'Installing a SMETS1 Electricity Meter' for relevant GroupID and shall take place in the order specified in that Table.

Error code on failure	S1SP checks and processing	DCO checks and processing	SupportingData
	Should any of the following checks fail, checking and processing in relation to that SMETS1 Installation shall not proceed to a subsequent step.		
ET01	For each of the CHF, GPF (for GroupID = AA, only where a GSMEDetail element is also present) and ESME, confirm that reading of the Public Application Association returns valid data, including all the device counters required by the subsequent steps in this table.		DeviceID

Error code on failure	S1SP checks and processing	DCO checks and processing	SupportingData
ET02	For each EncryptedMasterKey for this SMETS1 Installation, request that the DCO process the EncryptedMasterKey, and where that is successful, store the digitally signed package provided in response.	Confirm that the details provided are semantically identical to the corresponding EncryptedMasterKey in the corresponding Migration Group Encrypted File. Decrypt the EncryptedKey, re-encrypt that key with a secret key known only to the DCO, package that re-encrypted key with relevant Device IDs from the Migration Common File, then digitally sign and pass back the signed package to the S1SP .	EncryptedMasterKey
ET03	NOT USED		
ET04	Using the AuthenticationKey and EncryptionKey in each of the DataCollectionAssociation, ManagementAssociation and FirmwareAssociation within each of the CHFDetails, GPFDetails (for GroupID = AA, only where a GSMEDetail element is also present) and ESMEDetails: 1. confirm the successful creation of an Application Association with the Device in question, 2. close each such Application Association 3. securely store each key and its association with: o Its 'key type' o the 'name of Application Association' o the Device ID For clarity, this is to confirm that all keys operate before any are changed.		DeviceID || 'name of Application Association' Where 'name of Application Association' is one of DataCollectionAssociation, ExtendedDataCollectionAssociation, ManagementAssociation or FirmwareAssociation
ET05	Using the AuthenticationKey and EncryptionKey in the ExtendedDataCollectionAssociation in the CHFDetails: 1. confirm the successful creation of an Application Association with the Device, 2. read the CHF Whitelist, 3. confirm the Device ID for ESME is included in CHF Whitelist where the GroupID = AA, 4. read the serial number of the Device, 5. confirm the serial number of the Device is same as in SerialNumbers\CHF element for the SMETS1 Installation in Migration Group File 6. close the Application Association 7. securely store each key and its association with: o its 'key type' o the 'name of Application Association' o the Device ID o the serial number of the Device		1, 2, 3, 4, 5, 6 or 7 reflecting the sub step which failed

Error code on failure	S1SP checks and processing	DCO checks and processing	SupportingData
ET06	Using the AuthenticationKey and EncryptionKey in the ExtendedDataCollectionAssociation in the GPFDetails (for GroupID = AA, only where a GSMEDetail element is also present): 1. confirm the successful creation of an Application Association with the Device, 2. NOT USED 3. close the Application Association 4. securely store each key and its association with: a. its 'key type' b. the 'name of Application Association' c. the Device ID		1, 2, 3 or 4 reflecting the sub step which failed

ET07	Using the AuthenticationKey and EncryptionKey in the ExtendedDataCollectionAssociation in the ESMEDetails: 1. confirm the successful creation of an Application Association with the Device, 2. read the serial number of the Device, 3. confirm the serial number of the Device is same as in SerialNumbers\ESME element for the SMETS1 Installation in Migration Group File 4. read the Payment Mode (with its SMETS1 meaning) 5. if the Payment Mode is prepayment (with its SMETS1 meaning), read the UTRN Meter ID form the Device. 6. then close the Application Association 7. securely store each key and its association with: a. its 'key type' b. the 'name of Application Association' c. the Device ID d. the serial number of the Device 8. If the Payment Mode is prepayment (with its SMETS1 meaning): a. for SMETS1 Installations where the GroupID = BA, confirm the following are present and populated validly within the ESMEDetail of the DecryptedS1SPGroupInformation for the entry with the CHFIdentifier for this SMETS1 Installation: • PrepaymentKey • WrappedPrepaymentKey b. for SMETS1 Installations where the GroupID = CA, confirm the following are present and populated validly within the ESMEDetail of the DecryptedS1SPGroupInformation for the entry with the CHFIdentifier for this SMETS1 Installation: • PrepaymentKey • PrepaymentWrapperKey else if the Payment Mode is Credit (with its SMETS1 meaning): a. for SMETS1 Installations where the GroupID = CA or CB, if PrepaymentWrapperKey is present and populated validly within the ESMEDetail of the DecryptedS1SPGroupInformation for the entry with the CHFIdentifier for this SMETS1 Installation, securely store the PrepaymentWrapperKey and its association to the ESME Device ID. If the Payment Mode is prepayment (with its SMETS1 meaning), using the AuthenticationKey and EncryptionKey in the ManagementAssociation in the ESMEDetails: 9. confirm the successful creation of an Application Association with the Device,		1, 2, 3, 4, 5, 6, 7, 8, 9 ,10, 11, 12, 13 or 14 reflecting the sub step which failed

Error code on failure	S1SP checks and processing	DCO checks and processing	SupportingData
	10. create and send a zero value 'Add Credit' instruction, 11. confirm receipt of a successful response from the Device, 12. close the Application Association, 13. securely store the PrepaymentKey, PrepaymentWrapperKey and its association to the ESME Device ID, 14. set PrepayFlag attribute as true for the SMETS1 Installation in the S1SP Commissioning File		

Table A2

Installing a SMETS1 GSME

A3 The processing at Table A3 shall be that required of the S1SP and DCO for 'Installing a SMETS1 GSME' for this GroupID.

Error code on failure	S1SP checks and processing	DCO checks and processing	SupportingData
	Should any of the following checks fail, checking and processing in relation to that SMETS1 Installation shall not proceed to a subsequent step		
GT01	Using the DeviceID for the CHF on which the GSME should have been whitelisted: 1. Retrieve the AuthenticationKey and EncryptionKey for the Extended Data Collection Application Association 2. Using those keys, confirm the successful creation of an Application Association with the Device, 3. read the CHF Whitelist 4. confirm that the GSME's Device ID is on that CHF Whitelist and that the GSME has communicated in the last 24 hours, 5. close the Application Association		1, 2, 3, 4, or 5 reflecting the sub step which failed

Error code on failure	S1SP checks and processing	DCO checks and processing	SupportingData
GT02	Using the Device ID of the GPF associated with the GSME 1. Retrieve the AuthenticationKey and EncryptionKey for the Extended Data Collection Application Association 2. Using those keys, confirm the successful creation of an Application Association with the Device, 3. read the serial number of the Device, 4. for SMETS1 Installations where the GroupID = BA only, confirm the serial number of the Device is same as in SerialNumbers\ESME element for the SMETS1 Installation in Migration Group File, 5. read the Payment Mode (with its SMETS1 meaning) 6. if the Payment Mode is prepayment (with its SMETS1 meaning), read the UTRN Meter ID form the Device. 7. then close the Application Association 8. securely store the serial number of the Device and its association to the GSME Device ID 9. If the Payment Mode is prepayment (with its SMETS1 meaning): a. for SMETS1 Installations where the GroupID = BA, for the GSME identified in the GSMEIdentifier for this SMETS1 Installation in the Migration Common File, confirm the following are present and populated validly within the DecryptedS1SPGroupInformation for the GSMEDetails within the entry with the CHFIdentifier for this SMETS1 Installation: • PrepaymentKey • WrappedPrepaymentKey b. for SMETS1 Installations where the GroupID = CA or CB, for the GSME identified in the GSMEIdentifier for this SMETS1 Installation in the Migration Common File, confirm the following are present and populated validly within the DecryptedS1SPGroupInformation for the GSMEDetails within the entry with the CHFIdentifier for this SMETS1 Installation: • PrepaymentKey • PrepaymentWrapperKey else if the Payment Mode is Credit (with its SMETS1 meaning): a. for SMETS1 Installations where the GroupID = CA or CB, if either of the following are present and populated validly within the GSMEDetail of the DecryptedS1SPGroupInformation for the entry with the CHFIdentifier for this SMETS1 Installation, securely store with its association to the GSME Device ID: • PrepaymentWrapperKey • WrappedPrepaymentKey If the Payment Mode is prepayment (with its SMETS1 meaning), using the AuthenticationKey and EncryptionKey in the ManagementAssociation of the GPFDetail of the GPF associated with the GSMEDetails: 10. confirm the successful creation of an Application Association with the Device, 11. create and send a zero value 'Add Credit' instruction, 12. confirm receipt of a successful response from the Device 13. close the Application Association 14. securely store the PrepaymentKey, PrepaymentWrapperKey and its association to the GSME Device ID 15. set PrepayFlag attribute as true for the SMETS1 Installation in S1SP Commissioning File.		1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14 or 15 reflecting the sub step which failed

Table A3

Installing a SMETS1 PPMID

A4 The processing at Table A4 shall be that required of the S1SP and DCO for 'Installing a SMETS1 PPMID' for this GroupID.

Error code on failure	S1SP checks and processing	DCO checks and processing	SupportingData
	Should any of the following checks fail, checking and processing in relation to that SMETS1 Installation shall not proceed to a subsequent step		
	NOT USED		

Table A4

Commission Device (CHF)

A5 The processing at Table A5 shall be that required of the S1SP and DCO for 'Commission Device (CHF)' for this GroupID.

Error code on failure	S1SP checks and processing	DCO checks and processing	SupportingData
DP01	Instruct the DCC to add the relevant CHF details to the Smart Metering Inventory.		

Table A5

Securing a SMETS1 ESME

A6 The checks and processing at Table A6 shall be that required of the S1SP and DCO for 'Securing a SMETS1 ESME' for relevant GroupID and shall take place in the order specified in that Table.

Error code on failure	S1SP checks and processing	DCO checks and processing	SupportingData
	Should any of the following checks fail, checking and processing in relation to that SMETS1 Installation shall not proceed to a subsequent step		
ET08	For each EncryptedMasterKey for this SMETS1 Installation that relates to an ESME and / or CHF and / or (where a GSMEDetail element is also present) GPF: 1. Generate a new value for the EncryptionKey for the DataCollectionAssociation for one of the Devices within EncryptedMasterKey 2. Request that the DCO creates, using the relevant Master Key, the relevant form of the EncryptionKey for inclusion in key change instructions to the Device 3. Request that the Device changes to use the new key in this Application Association 4. Confirm that the Device has switched to using the new key 5. securely store the new key and its association with: o its 'key type' o the 'name of Application Association' o the Device ID 6. invalidate the replaced key	Create the relevant form of key required for inclusion in the instructions using the relevant Master Key.	DeviceID, so identifying the Master Key which is not functioning

Table A6

Appendix B **Device Installation – For GroupID EA, EB, EC**

Placeholder for FOC

Appendix C **Device Installation – For GroupID DA**

Installing a SMETS1 Electricity Meter

C1 The checks and processing at Table C1 shall be that required of the DCC for 'Installing a SMETS1 Electricity Meter' and shall take place in the order specified in that Table.

Error code on failure	DCC checks and processing	SupportingData
	Should any of the following checks fail, checking and processing in relation to that SMETS1 Installation shall not proceed to a subsequent step.	

Error code on failure	DCC checks and processing	SupportingData
ET01	Using the DeviceID for the ESME: 1. read the Payment Mode (with its SMETS1 meaning); and 2. ensure the VendPriceChangeHANLimit is set to zero. If the Payment Mode is prepayment (with its SMETS1 meaning): 3. create and send a zero value 'Add Credit' instruction, 4. confirm receipt of a successful response from the Device, 5. store the PrepayFlag attribute as true for the SMETS1 Installation for the S1SP Commissioning File generation.	1, 2, 3, 4 or 5 reflecting the sub step which failed

Table C1

Installing a SMETS1 GSME

C2 The processing at Table C2 shall be that required of the DCC for 'Installing a SMETS1 GSME' and shall take place in the order specified in that Table.

Error code on failure	DCC checks and processing	SupportingData
	Should any of the following checks fail, checking and processing in relation to that SMETS1 Installation shall not proceed to a subsequent step	
GT01	Using the DeviceID for the CHF on which the GSME should have been whitelisted: 1. read the CHF Whitelist and 2. confirm that the GSME's Device ID is on that CHF Whitelist and that the GSME has communicated in the last 24 hours.	
GT02	Using the Device ID of the GPF associated with the GSME 1. read the Payment Mode (with its SMETS1 meaning) 2. ensure the VendPriceChangeHANLimit is set to zero. If the Payment Mode is prepayment (with its SMETS1 meaning): 3. create and send a zero value 'Add Credit' instruction, 4. confirm receipt of a successful response from the Device 5. store the PrepayFlag attribute as true for the SMETS1 Installation for the S1SP Commissioning File generation.	1, 2, 3, 4, or 5 reflecting the sub step which failed

Table C2

Installing a SMETS1 PPMID

C3 No additional checks or processing is required.

Commission Device (CHF)

C4 The processing at Table C4 shall be that required of the S1SP for 'Commission Device (CHF)'.

Error code on failure	S1SP checks and processing	DCO checks and processing	SupportingData
DP01	Instruct the DCC to add the relevant CHF details to the Smart Metering Inventory.	None required	

Table C4

Securing a SMETS1 GSME

C5 The checks and processing at Table C5 shall be that required of the S1SP and DCO for 'Securing a SMETS1 GSME' for the relevant GroupID and shall take place in the order specified in that Table.

Error code on failure	S1SP checks and processing	DCO checks and processing	SupportingData
	Should any of the following checks fail, checking and processing in relation to that SMETS1 Installation shall not proceed to a subsequent step, except where otherwise stated.		

Error code on failure	S1SP checks and processing	DCO checks and processing	SupportingData
GT03	The S1SP shall request using the GSME serial number that the DCO creates a Single Use Authorisation Code for SUAKeyDetails for the Device type GSME to bring the GSME within DCO control.	The DCO validates that serial number is currently in a DCO Viable Installation, and if so creates an authorisation instruction, containing a DCO Public Key, using the decrypted EncryptedSUAKey element, and then persists relevant information about the SMETS1 Installation.	
GT04	The S1SP shall send the authorising instruction to the GSME requesting that it performs a key rotation to come under the DCO control.	None required	
GT05	If the S1SP receives a response from the GSME indicating a success of the authorising instruction from the DCO pursuant to GT04, then the S1SP shall store: 1. the DCO Public Key; and 2. the GSME's Public Key generated as a result of this instruction and the associated Digital Signature created using the GSME's permanent Private Key.	None required	1 or 2 reflecting the sub step which failed
GT06	If the S1SP receives a response from the GSME indicating a failure of the authorising instruction from the DCO, the S1SP shall: 1. read the GSME's Public Key and the associated Digital Signature from the GSME; 2. request using the GSME serial number, the GSME's Public Key and the DCO Public Key that the DCO creates an authorising instruction to rotate the key used to authenticate instructions to the GSME; 3. sends the authorising instruction to the GSME requesting that it performs a key rotation to change the key used to authenticate instructions from the DCO.	The DCO validates the Digital Signature on the GSME public key against the Public Key stored from the installation. The DCO creates an authorisation instruction, containing a DCO Public Key, using the key derived from the GSME's Public Key and the Private Key corresponding to the supplied DCO Public Key.	1, 2 or 3 reflecting the sub step which failed
GT07	If the S1SP receives a response from the GSME indicating a success of the authorising instruction from the DCO pursuant to GT04, then the S1SP shall store: 1. the DCO Public Key; and 2. the GSME's Public Key generated as a result of this instruction and the associated Digital Signature created using the GSME's permanent Private Key.	None required	1 or 2 reflecting the sub step which failed

Table C5

Securing a SMETS1 ESME

C6 The checks and processing at Table C6 shall be that required of the S1SP and DCO for 'Securing a SMETS1 ESME' for the relevant GroupID and shall take place in the order specified in that Table.

Error code on failure	S1SP checks and processing	DCO checks and processing	SupportingData
	Should any of the following checks fail, checking and processing in relation to that SMETS1 Installation shall not proceed to a subsequent step, except where otherwise stated		
ET03	The S1SP shall request using the ESME serial number that the DCO creates a Single Use Authorisation Code for SUAKeyDetails for the Device type ESME to bring the ESME within DCO control.	The DCO validates that serial number is currently in a DCO Viable Installation, and if so creates an authorisation instruction, containing a DCO Public Key, using the decrypted EncryptedSUAKey element, and then persists relevant information about the SMETS1 Installation.	
ET04	The S1SP shall send the authorising instruction to the ESME requesting that it performs a key rotation to come under the DCO control.	None required	
ET05	If the S1SP receives a response from the ESME indicating a success of the authorising instruction from the DCO pursuant to ET04, then the S1SP shall store: 1. the DCO Public Key; and 2. the ESME's Public Key generated as a result of this instruction and the associated Digital Signature created using the ESME's permanent Private Key.	None required	1 or 2 reflecting the sub step which failed

Error code on failure	S1SP checks and processing	DCO checks and processing	SupportingData
ET06	If the S1SP receives a response from the ESME indicating a failure of the authorising instruction from the DCO, the S1SP shall: 1. read the ESME's Public Key and the associated Digital Signature from the ESME; 2. request using the ESME serial number, the ESME's Public Key and the DCO Public Key that the DCO creates an authorising instruction to rotate the key used to authenticate instructions to the ESME; 3. sends the authorising instruction to the ESME requesting that it performs a key rotation to change the key used to authenticate instructions from the DCO.	The DCO validates the Digital Signature on the ESME public key against the Public Key stored from the installation. The DCO creates an authorisation instruction, containing a DCO Public Key, using the key derived from the ESME's Public Key and the Private Key corresponding to the supplied DCO Public Key.	1, 2 or 3 reflecting the sub step which failed
ET07	If the S1SP receives a response from the ESME indicating a success of the authorising instruction from the DCO pursuant to ET03, then the S1SP shall store: 1. the DCO Public Key; and 2. the ESME's Public Key generated as a result of this instruction and the associated Digital Signature created using the ESME's permanent Private Key.	None required	1 or 2 reflecting the sub step which failed

Table C6