Version 0.1

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 the TMAD and submit it to the Secretary of State in accordance with the process set out in Section N6.4 of the Code.

2 Defined Terms

Term	Meaning
Active Device	Shall mean an Active Meter or Active GPF as the context requires.
Active Device Authorisation File	Shall mean a file created by a Responsible Supplier for one or more SMETS1 Installations that complies with requirements of Clause 4.20
Active GPF	Shall mean the SMETS1 GPF that is associated with an SMETS1 GSME that is an Active Meter.
Active Meter	Shall mean, at the relevant point in time, a SMETS1 ESME or SMETS1 GSME in relation to which, at that point in time, the Responsible Supplier has arrangements with a SMETS1 SMSO to provide its 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 4.
Authorised DCO SMETS1 Device Credentials	Shall have the meaning set out in the SMETS1 Supporting Requirements.
Authorised S1SP SMETS1 Device Credentials	Shall have the meaning set out in the SMETS1 Supporting Requirements.

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 only includes the Device ID for an ESME where that ESME communicates with the CHF using a ZigBee network. The CHF Whitelist, for Group IDs specified at Section 12, 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 3 to guard against replay of files processed pursuant to this TMAD.
Commissioning Party	See Clause 3.1.
Commissioning Party Systems	See Clause 3.1.
Commissioning Request	Shall mean a request from the Commissioning Party for one of the Services listed in the DUIS.
Common Validation Checks	Shall means those checks carried out pursuant to Clause 5.10.

Term	Meaning
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.
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.
DCC's Microsoft SharePoint	A web-based collaborative platform that DCC uses to share and exchange information with individual SEC Parties. This allows information to be shared securely between a specific SEC Party and a specific part of DCC Live Systems.
DCO Required File Set	Shall mean the set of files specified at Section 12 for the relevant GroupID.
DCO Viable Installations	Shall have the meaning ascribed to that term in Clause 5.19.
Dormant Meter	Shall mean a SMETS1 ESME or a SMETS1 GSME that is installed in respect of an Energy Consumer's premises and is: i) configured so as to be capable of remote communication with a SMETS1 SMSO via a SMETS1 CHF; and ii) not an Active Meter.
Group	Shall mean the set of SMETS Installations identified by the same Group ID on the Group Device Model Combination List.

Term	Meaning
Group Device Model Combination List	For each Group, the combinations of Device Models (where each combination comprises an entry on the SMETS1 Eligible Product Combinations) associated with that Group ID.
Group ID	Shall be the unique value used to identify a Group within the Group Device Model Combination List.
IEEE	The Institute of Electrical and Electronics Engineers.
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.
Migration	See Clause 3.1(c).
Migration Authorisation	An authorisation given by the Responsible Supplier in relation to a SMETS1 Installation pursuant to the Migration Authorisation Mechanism to commence the Migration of a SMETS1 Installation.
Migration Authorisation Mechanism	The mechanism of that name referred to in Clause 4.20.
Migration Common File	Shall mean a file created by a Requesting Party pursuant to Clause 5.8 that details information about SMETS1 Installations, which would be required for any SMETS1 Installations regardless of Group.
Migration Common File Counter	A counter of that name created and maintained pursuant to Table 3 to guard against replay of relevant files processed pursuant to this TMAD.
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.

Term	Meaning
Migration Common Validation File Counter	A counter of that name created and maintained pursuant to Table 3 to guard against replay of relevant files processed pursuant to this TMAD.
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, where required for the Group identified by Group ID, any additional, Group specific information required by Section 12 onwards[1]. For clarity, such relevant files shall only be processed where they are specified as being required at Section 12.
Migration Group Encrypted File Counter	A counter of that name created and maintained pursuant to Table 3 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 Group ID, any additional, Group-specific information required by Section 12.
Migration Group File Counter	A counter of that name created and maintained pursuant to Table 3 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.
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.

[1] Section 12 onwards will be updated with Group specific details when these become known for each Group.

Term	Meaning
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.
Requested Installations	Shall have the meaning ascribed to that term in Clause 5.12.
Requesting Party	See Clause 3.1.
Requesting Party Systems	See Clause 3.1.
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.
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 3 to guard against replay of files processed pursuant to this TMAD.

Term	Meaning
S1SP Required File Set	Shall mean the set of files specified at Section 12 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 Installation	See Clause 3.1.
SMETS1 Migration Interface	Shall be the technical interface, as specified at Clause 9, allowing 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 Section 10.
Supplier Certificate ID	The Certificate ID of an Organisation Certificate that has been Issued to a Supplier Party.

2.2 The XML elements listed in

KeyInfo	Shall contain an X509IssuerSerial element (in a single X509Data element) which shall identify the Organisation Certificate that can be used to Check Cryptographic Protection

2.3 Table 12 are references to the parts of the SMETS1 Migration Schema, and shall have the meaning given to them in

KeyInfo	Shall contain an X509IssuerSerial element (in a single X509Data element) which shall identify the Organisation Certificate that can be used to Check Cryptographic Protection

2.4 Table 12 and 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.

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

3 Transitional Application of Sections of the Code

Application of Section A

3.1 Whilst this TMAD remains in force, Section A of the Code shall apply as follows:

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

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) or (j) below) processing 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) Threshold Anomaly Detection and (other than to the extent to which the activity falls within paragraph (d) or (f) below) Cryptographic Processing relating to the generation and use of a Message Authentication Code;

(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 (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 the part used for each other such purpose; (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 the part used by each other SMETS1 Service Provider; (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 the part used by each other DCO; and (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 the part used by each other Requesting Party.

(c) Words beginning with capital letters which are defined in the Transition and Migration Approach Document shall, unless the context otherwise requires, have the meanings given to them in the Transition and Migration Approach Document. In particular, 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.
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.
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 TMAD) shall not be considered to form part of the Requesting Party Systems.
SMETS1 Installation	Shall be 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 which are authorised to communicate over the ZigBee network to which the CHF controls access. The set of other Devices may include at most one SMETS1 GSME, at most one SMETS1 PPMID, at most one SMETS1 IHD and at most one SMETS1 CAD.

(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 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.

Application of Section F

3.2 Whilst this TMAD remains in force, for the purposes of Section F2.10A, 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, additionally identify, in relation to that entry, the SMETS1 SMSO and the provider of communications services. Where either list contains two or more entries that have the same combination of Device Models but identify different SMETS1 SMSOs, each entry shall be treated as a separate entry for the purpose of the list.

3.3 The DCC shall not add an entry to the list of SMETS1 Eligible Product Combinations other than to the extent that it has approval of the Secretary of State to do so.

Application of Section G

3.4 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.

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

3.6 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.

3.7 The DCC shall ensure that Anomaly Detection Thresholds set in relation to the Commissioning Party are 0 for all requests that are not identified in Table 9 of this TMAD.

Application of Section H3.22

3.8 Within 5 Working Days after this TMAD comes into effect, each User shall provide the DCC with an additional forecast under Section H3.22 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.

Application of the Inventory Enrolment and Decommissioning Procedures

3.9 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 are not Associated (or to be Associated) with a Smart Metering System that has been Enrolled. Instead, no Party shall seek to add any such SMETS1 Device to the Smart Metering Inventory other than:

i) in the case of such a SMETS1 CHF, an S1SP in the circumstances set out in the SMETS1 Supporting Requirements; or

ii) in the case of any other such SMETS1 Device, the Responsible Supplier for the Device or the Commissioning Party and, 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 5.26 without any failures flagged as 'Critical'.

[DN: please note that it is proposed that the IEDP will be further updated to include post-commissioning obligations on DCC in respect of SMETS1 Devices which will include in relation to the initial Groups an obligation to update various security keys].

Application of Section L

3.10 Whilst this TMAD remains in force, Section L of the Code shall be modified as follows:

(a) The table in Section L3.18 shall be amended to include the following additional rows:

Remote Party Role	**Party**	**User Role or RDP**	**DCC Live Systems definition paragraph**
commissioningPartyFileSigning	The DCC	[Not Applicable]	(j)
requestingPartyFileSigning	The DCC	[Not Applicable]	(i)
s1SPMigrationSigning	The DCC	[Not Applicable]	(h)
commissioningPartyXmlSigning	The DCC	[Not Applicable]	(j)

(b) The table in Section L3.18 shall be amended to include the following additional rows:

Remote Party Role	**Remote Party Role Code**
commissioningPartyFileSigning	132

requestingPartyFileSigning	131
s1SPMigrationSigning	130
commissioningPartyXmlSigning	133

Application of Section M

3.11 The Responsible Supplier for each [Device referred to in Clause 4.14 of the Transition Migration Approach Document] acknowledges that the carrying out of any of the steps referred to in [Clauses 4.14 and 4.15] of the Transition Migration Approach Document 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. Provided that the DCC undertakes those steps in accordance with this Code, neither the DCC nor the SMETS1 SMSOs shall be liable to the Responsible Supplier (or any other Supplier Party) for any such loss of Data or functionality that arises from the carrying out of, or from any attempt to carry out, any of those steps.

3.12 Where a Supplier Party agreed with a SMETS1 SMSO that the SMETS1 SMSO would 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 the Transition and Migration Approach Document in order to Migrate that SMETS1 Installation. The SMETS1 SMSOs shall be entitled to rely on this confirmation under Section M11.5 of the Code.

3.13 It is acknowledged that each SMETS1 SMSO is (including when acting on behalf of the DCC in its capacity of Requesting Party), when undertaking the steps assigned to it in the Transition Migration Approach Document, acting as a DCC Service Provider, and is therefore entitled to rely on the waiver and release in Section M2.13(a) of the Code and the third party rights under Section M11.5 of the Code.

4 Pre-Migration Rights and Obligations

Scheduling and pre-conditions for Migration

4.1 Each Supplier Party shall provide any information that the DCC reasonably requests in order to support the planning, coordination, 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 The Requesting Party shall not commence the Migration of any SMETS1 Installation that does not comprise Devices that correspond to an entry on the SMETS1 Eligible Product Combination.

4.3 The Requesting Party shall not commence the Migration of any SMETS1 Installation until it has received (and/or is deemed to have received in accordance with Clause 4.15) a Migration Authorisation from the Responsible Supplier or Responsible Suppliers for that SMETS1 Installation.

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

4.5 Subject to Clauses 4.2 and 4.3 the Requesting Party shall take reasonable steps to initiate the Migration of a SMETS1 Installation in timescales consistent with those requested by the Responsible Supplier(s) for any Active Meters within that SMETS1 Installation.

4.6 Subject to Clause 4.2 and 4.3 where there is more than one Responsible Supplier for a SMETS1 Installation, the Requesting Party shall take reasonable steps to initiate the Migration of that SMETS1 Installation in timescales that are consistent with the later of those established with each Responsible Supplier.

4.7 The Requesting Party shall ensure that the Responsible Supplier for an Active Meter is provided with any information that is reasonably relevant to the timing of when the Migration of the SMETS1 Installation of which the Active Meter forms a part will occur, no later than [21 days] prior to such Migration.

4.8 In the event that there is any disagreement between the DCC and any Responsible Supplier for an Active Meter that comprises part of a SMETS1 Installation over the timing of the initiation of the Migration of that SMETS1 Installation, the Responsible Supplier may refer the matter to the Secretary of State for a determination (and the Secretary of State's decision will be binding for the purposes of the Code).

4.9 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.

4.10 The DCC shall, from time to time, use and rely upon the information provided to it by SMETS1 SMSOs 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.

4.11 The DCC shall have no liability to any Party where it Migrates (or does not Migrate) a SMETS1 Installation in circumstances where it should not (or should) have done so, to the extent that the same arises due to inaccuracies in the information referred to in Clause 4.10 that are not caused by the DCC.

4.12 The TMAD constitutes each Responsible Supplier's documented instructions to the DCC to Process any Personal Data required for the purposes of Enrolment of SMETS1 Smart Metering Systems.

Dormant Meters

4.13 Each Responsible Supplier for each SMETS1 CHF that forms part of a SMETS1 Installation that comprises one or more Dormant Meters agrees that the relevant SMETS1 SMSO may 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.

4.14 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, for the purposes of preparing for the Migration of any such SMETS1 Installation in accordance with the provisions of this TMAD, take any steps reasonably necessary in order to ensure that the Device is configured in accordance with the

requirements of Clauses 5.12(d) and 5.12(e), including upgrading the firmware on the Device for that purpose.

4.15 Subject to Clause 4.16, the Responsible Supplier for each Device referred to in Clause 4.14, 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.

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

4.17 Where there is no Active Meter forming part of the same SMETS1 Installation as a SMETS1 Device referred to in Clause 4.14, the DCC shall take reasonable steps to notify the Responsible Supplier for such Devices at least 21 days before it carries out any of the steps referred to in that Clause.

4.18 Where there is no Active Meter forming part of the same SMETS1 Installation as a SMETS1 Device referred to in Clause 4.14, the DCC shall take reasonable steps to notify the Responsible Supplier for such Devices at least 21 days before it carries out any of the steps referred to in that Clause.

4.19 The Installing Supplier for each Device referred to in Clause 4.14 shall provide such support and assistance as the DCC may reasonably request (including, where available to that Supplier Party, provision of new 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 4.14.

Migration Authorisation

4.20 No later than 7 days following the coming into effect of this TMAD, the DCC shall set out and make available to all Supplier Parties the proposed mechanism by which:

(a) a Migration Authorisation may be provided by the Responsible Supplier(s) for a SMETS1 Installation to the Requesting Party; and

(b) where the Responsible Supplier is the Responsible Supplier for all Devices comprising a SMETS1 Installation, the Responsible Supplier may indicate whether it wishes the Commissioning Party to carry out the steps necessary to Commission the Devices comprising that SMETS1

Installation or, alternatively that it wishes itself to carry out these steps,

the "Migration Authorisation Mechanism".

4.21 The Migration Authorisation Mechanism shall require that the Responsible Supplier(s) for a SMETS1 Installation for which 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 1 shall provide the information required in that table for that Device.

Device	**Required information**
SMETS1 ESME	CriticalSupplierCertificateID NonCriticalSupplierCertificateID
SMETS1 GPF	CriticalSupplierCertificateID NonCriticalSupplierCertificateID
SMETS1 GSME	CriticalSupplierCertificateID NonCriticalSupplierCertificateID

Table 1

4.22 The Migration Authorisation Mechanism shall require the Responsible Supplier 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.

4.23 Within one calendar month of carrying out the steps referred to in Clause 4.20 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.

4.24 Following DCC's publication of the Migration Authorisation Mechanism and in accordance with the requirements of Clause 4.23 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 [and the Secretary of State's decision will be binding for the purposes of the Code].

4.25 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 time. The processes set out in Clauses 4.23 and 4.24 shall apply to any modification of the Migration Authorisation Mechanism.

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, publish to the SMETS1 SMSO:

(a) where SMETS1 Installations for that Group, according to Section 12, require a Migration Group Encrypted File, the Public Keys that are to be

used to create any required S1SPEncryptedKey or EncryptedMasterKey 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 that would be required in order to configure Devices within such SMETS1 Installations and any associated systems, 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 EncryptedMasterKey elements, shall be generated by, and known only to, the DCO which has the capability to operate associated DCC functions in relation to SMETS1 Installations within the relevant Group.

5.4 Any Private Key, which is associated with a Public Key published pursuant to Clause 5.1 for use in creating S1SPEncryptedKey elements, shall be generated by, and known only to, the S1SP which has the capability to operate associated DCC functions in relation to SMETS1 Installations within the relevant Group.

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 2. The Parties identified in Table 2 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
Where required by the DCC, a file containing Migration Authorisations	Supplier Party	supplierMigrationFileSigning

Table 2

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 3 so that the files each creates shall, except in cases of replay, pass the anti-replay checks specified in Table 4

5.7 Where an entity acts as the Authenticator with respect to the checks and processing required by Table 4, it shall have the capacity to establish and

maintain the counters in the 'Counter of Authenticator' column of Table 3 in the way required by Table 4.

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 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 3

Creation and validation of standard information

5.8 Before the Migration of any set of SMETS1 Installations is triggered pursuant to Clause 5.9, the Requesting Party shall validate that they could potentially be successfully Migrated. To this end, 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. In such files, the value for 'ToBeCommissionedByDCC' may only be set to 'False' if all of the Supplier Certificate IDs within it refer to Certificates all of which contain User IDs allocated to the same Supplier Party. 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.

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 4 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.
1	Confirm the xml file is well formed and valid against the SMETS1 Migration Schema and meets the requirements of Clause 10.1
2	Check Cryptographic Protection in terms of the signature within the file
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 2 for the relevant file type
4	Confirm Validity of the Certificate used to Check Cryptographic Protection at Step Number 2
5	Where the file is a Migration Common File confirm either that: 1. the Authenticator holds a Migration Common File Stored Counter for the Requesting Party Identifier (RequestingPartyID) and the MCFCounter is greater than that Migration Common File Stored Counter; or 2. the Authenticator does not hold a Migration Common File Stored Counter for this Requesting Party Identifier Should this check succeed, the Authenticator shall: 1. If it does not hold a Migration Common File Stored Counter for this Requesting Party Identifier (RequestingPartyID), create such a Migration Common File Stored Counter; and 2. In all cases, set the Migration Common File Stored Counter to the value of MCFCounter
6	Where the file is a Migration Group File confirm either that: 1. the Authenticator holds a Migration Group File Stored Counter for this Requesting Party Identifier (RequestingPartyID) and the MGFCounter is greater than that Migration Group File Stored Counter; 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. If it does not hold a Migration Group File Stored Counter for this Requesting Party Identifier (RequestingPartyID), create such a Migration Group File Stored Counter; and 2. In all cases, set the Migration Group File Stored Counter to the value of MGFCounter.
7	Where the file is a Migration Group Encrypted File confirm either that: 1. the Authenticator holds a Migration Group Encrypted File Stored Counter for this Requesting Party Identifier (RequestingPartyID) and the MEFCounter is greater than that Migration Group Encrypted File Stored Counter; 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. If it does not hold a Migration Group Encrypted File Stored Counter for this Requesting Party Identifier (RequestingPartyID), create such a Migration Group File Stored Counter; and 2. In all cases, set the Migration Group Encrypted File Stored Counter to the value of MEFCounter.
8	Where the file is a Migration Common Validation File confirm either that:

Step number	Checks and processing
	1. the Authenticator holds a Migration File Common Validation Stored Counter for this Requesting Party Identifier (RequestingPartyID) and the MVFCounter is greater than that Migration File Common Validation Stored Counter; 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: 3. If it does not hold a Migration File Common Validation Stored Counter for this Requesting Party Identifier (RequestingPartyID), create such a Migration File Common Validation Stored Counter; and 4. In all cases, set the Migration File Common Validation Stored Counter to the value of MVFCounter.
9	Where the file is a S1SP Commissioning File confirm either that: 1. the Authenticator holds a S1SP Commissioning File Stored Counter for this S1SP Identifier (S1SPID) and the SCFCounter is greater than that S1SP Commissioning File Stored Counter; 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. If it does not hold a S1SP Commissioning File Stored Counter for this S1SP Identifier (S1SPID), create such a S1SP Commissioning File Stored Counter; and 2. In all cases, set the S1SP Commissioning File Stored Counter to the value of SCFCounter.
10	If 'ToBeCommissionedByDCC' is set to 'False', all of the Supplier Certificate IDs refer to Certificates all of which contain User IDs allocated to the same Supplier Party.

Table 4

5.10 Where all checks and processing at Clause 5.9 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;

(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. 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 (the 'FailedStepNumber') and (2) the SupportingData (as required by the relevant row in from Table 5). For clarity, the DCC shall undertake all checks from Table 2 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 SMETS1Installations 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
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 Certified Products List and that that CPL entry is for the required DeviceType	DeviceID of the Device whose Device Modell is not on the CPL
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
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 Group ID matches the GroupID in the file.	None
4	For the CHF then the ESME then the GSME (if present) then the PPMID (if present) then the IHD (if present) then the PPMID (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	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
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
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
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
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.	
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.	
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:
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
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
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.	
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
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:
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

Table 5

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 4 for such a file.

Preparing to trigger Migration

5.12 Where a Requesting Party wishes to Migrate one or more SMETS1 Installations (the 'Requested Installations'), and has secured the required Migration Authorisations for the Requested Installations, it shall first:

(a) ensure 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 and authenticated as required by Clause 5.11 within the prior 24 hours;

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

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

(d) ensure that all Devices within the Requested Installations have been configured as required by Clause 13 of the SMETS1 Supporting Requirements, where such configuration is required for this GroupID as specified in the 'Pre-enrolment Configuration Requirements' section of Section 12 for this GroupID; and

(e) ensure that all Devices within the Requested Installations, and any associated systems, have been configured in line with the requirements published by the DCC pursuant to Clause 5.1(b).

and shall then:

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

(g) if required by Section 12 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 S1SPEncryptedKey, EncryptedMasterKey and S1SPGroupInformation parts of a Migration Group Encrypted File shall be encrypted according to Section 11 where the Public Keys used are those published by DCC pursuant to Clause 5.1(a) for the Group ID in question.

S1SP and DCO receipt of migration data

5.13 Where the DCC receives a Migration Group Encrypted File, the DCC shall ensure 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 4 for such a file. The DCO shall then:

(a) attempt to decrypt the EncryptedMasterKey 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 Group ID in question; and

(b) ensure that the plaintext outputs from decrypting EncryptedMasterKey are well formed and valid against the SMETS1 Migration Schema for a DecryptedMasterKey structure.

If either 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 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 5.195.20, 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; and

(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 at Section 12.

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:

(a) either, 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 4 for such a file.

5.23 For a Migration Group Encrypted File, the S1SP shall then:

(a) attempt to decrypt the S1SPGroupInformation and S1SPEncryptedKey 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 Group ID in question; and

(b) ensure that the plaintext output from decrypting S1SPGroupInformation 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 6. 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 6 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
1.1	For each CHFIdentifier in the Migration Group File, ensure that the Migration Common File contains a CHFIdentifier with the same value
1.2	For each CHFIdentifier in the Migration Group File, ensure that the Migration Common Validation File does not contain a CHFIdentifier with the same value indicating a validation error
2.X	Under the steps required by 'S1SP Migration Group File data validation' for the specified GroupID, as detailed at Section 12, where X has the value specified at that Appendix
3.X	Under the steps required by 'S1SP Migration Group Encrypted File data validation' for the specified GroupID, as detailed at Section 12, where X has the value specified at that Appendix

Table 6

5.26 The S1SP shall treat only information which is (1) for an S1SP Viable Installation and (2) 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 'S1SP / DCO Commissioning of SMETS1 Installation' for the associated GroupID, as specified in Section 12;

(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 SMETS 1Installation via the relevant SMETS1 SMSO; and

(iii) undertake no further processing in relation to that SMETS1 Installation as part of the processing of that Migration Group File 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 SMETS1Installation'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

(b) either:

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

(d) 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, the Commissioning Party shall, as the Authenticator, undertake the sequence of checks and processing required by Table 4 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 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 7 values for the relevant Commissioning Request), as required by Table 7 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' 15 to 19, the Commissioning Party shall append to the SMETS1Installation element, a FailedCheck element which includes the relevant StepNumber from Table 7 (the 'FailedStepNumber'). For clarity (1) the Commissioning Party shall undertake all steps from 15 to 19 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 the Device is not present, a step cannot produce errors.

StepNumber	Commissioning Request	Only submit if:	Target SMETS1 Device ID	Other SMETS1 Device ID	RemotePartyRole
1.	Device Pre-notification	True	DeviceID in ESME	NA	NA
2	Update HAN Device Log	True	DeviceID in CHF	DeviceID in ESME	NA
3	Device Pre-notification	If GSME present	DeviceID in GSME	NA	NA
4	Update HAN Device Log	If GSME present	DeviceID in CHF	DeviceID in GSME	NA
5	Device Pre-notification	If PPMID present	DeviceID in PPMID	NA	NA
6	Update HAN Device Log	If PPMID present	DeviceID in CHF	DeviceID in PPMID	NA
7	Device Pre-notification	If IHD present	DeviceID in IHD	NA	NA
8	Update HAN Device Log	If IHD present	DeviceID in CHF	DeviceID in IHD	NA
9	Device Pre-notification	If CAD present	DeviceID in CAD	NA	NA
10	Update HAN Device Log	If CAD present	DeviceID in CHF	DeviceID in CAD	NA
11	Commission Device	True	DeviceID in ESME	NA	NA
12	Commission Device	If GSME present	DeviceID in GSME	NA	NA
13	Join Service (Critical)	If PPMID present	DeviceID in ESME	DeviceID in PPMID	NA
14	Join Service (Non-Critical)	If PPMID present	DeviceID in PPMID	DeviceID in ESME	NA
15	Join Service (Non-Critical)	If GSME present	DeviceID in GSME	DeviceID in GPF	NA
16	Request Handover Of DCC Controlled Device	If Supplier Certificate IDs in the ESME element are not null	DeviceID in ESME	NA	Supplier
17	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

StepNumber	Commissioning Request	Only submit if:	Target SMETS1 Device ID	Other SMETS1 Device ID	RemotePartyRole
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
19	Request Handover Of DCC Controlled Device	If Network Operator Certificate IDs in the ESME element are not null	DeviceID in ESME	NA	NetworkOperator
19	Request Handover Of DCC Controlled Device	If Network Operator Certificate IDs in the GPF element are not null	DeviceID in GPF	NA	NetworkOperator

Table 7

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 same for all 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 a Supplier Party is identified in the corresponding entries in the Migration Common File, the 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. For clarity, this would, for Smart Meters which are successfully commissioned, require that the S1SP issue corresponding SMETS1 'Device Commissioned' Alerts to the Responsible Supplier for that Smart Meter.

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.

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 six 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 7.3above, 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 above, 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 that have been Issued to:

(a) that Requesting Party; and

(b) any S1SP that pertains to any Group that pertains to that Requesting Party 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 above;

(b) revoke any Certificate associated with any other Public Key in addition to those referred to in Clause 7.7 above; 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 have been Issued to the Commissioning Party.

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 above;

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

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 11, 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 SMHAN.

8.6 The DCC shall additionally apply the validation checks in Table 8 to all Commissioning Requests that it receives from the Commissioning Party, and shall additionally apply the validation checks in Table 10 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 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 or Table 10 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 and Table 10 in the sequence they appear in each Table and shall successfully apply all Table 8 checks before applying checks in Table 10. 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	Error Handling Strategy procedure
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 9	E**[TBC]**	Commissioning Party is not allowed to use such Service Requests	Error	Acknowledgement	**[TBC]**
The Remote Party Role in the Certificate used to verify the Digital Signature on the Commissioning Request is that required by Table 2.	E**[TBC]**	Wrong Remote Party Role for Commissioning Request	Error	Acknowledgement	**[TBC]**
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	E**[TBC]**	Commissioning Party identifier mismatch in Commissioning Service Request	Error	Acknowledgement	**[TBC]**
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.	E**[TBC]**	Target is not a SMETS1 Device	Error	Acknowledgement	**[TBC]**
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	E**[TBC]**	Other Device is not a SMETS1 Device	Error	Acknowledgement	**[TBC]**

Table 8

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 9

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**	**Error Handling Strategy procedure**
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'.	E**[TBC]**	Remote Party Role in Certificates different than in request	Error	Acknowledgement	**[TBC]**
Request Handover Of DCC Controlled Device	Confirm that ExecutionDateTime is not present	E**[TBC]**	Cannot future date Commissioning Requests	Error	Acknowledgement	**[TBC]**
Request Handover Of DCC Controlled Device	Confirm that the Entity Identifiers in all Certificates contained within ReplacementCertificates are identifiers for the same Party.	E**[TBC]**	Not all identifiers are for the same Party	Error	Acknowledgement	**[TBC]**
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.	E**[TBC]**	Asserted Supplier is not the Supplier	Error	Acknowledgement	**[TBC]**

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	Error Handling Strategy procedure
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.	E**[TBC]**	Asserted Network Operator is not the Network Operator	Error	Acknowledgement	**[TBC]**
Update HAN Device Log	Confirm that ExecutionDateTime is not present.	E**[TBC]**	Cannot future date Commissioning Requests	Error	Acknowledgement	**[TBC]**
Update HAN Device Log	Confirm that RequestType is 'Add'.	E**[TBC]**	Commissioning Party cannot remove Devices	Error	Acknowledgement	**[TBC]**
Update HAN Device Log	Confirm that InstallCode is '00000000000000000000000000000000'	E**[TBC]**	Commissioning Party cannot install new Devices	Error	Acknowledgement	**[TBC]**

Table 10

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)	1
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 & RemotePartyPrepaymentTopUpFloorSeqNumber	Request Handover Of DCC Controlled Device	0 (zero)
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)
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

DUIS Data Item	Commissioning Service Request(s)	Value
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'; '1.2' otherwise
FirmwareVersion	Device Pre-Notification	As specified in relation to the 'Target SMETS1 Device ID'
ESMEVariant	Device Pre-Notification	Not present unless DeviceType = "ESME'; 'A' otherwise
AssociatedGPFDeviceID	Device Pre-Notification	Never present

Table 11

9 SMETS1 Migration Interface

9.1 This Clause 9 specifies the technical interface allowing the exchange of files between the DCC and DCC Users pursuant to such 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 each Supplier Party can exchange files relevant to them.

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 13. Each such XML structure shall be populated with information, within each element, as required by

KeyInfo	Shall contain an X509IssuerSerial element (in a single X509Data element) which shall identify the Organisation Certificate that can be used to Check Cryptographic Protection

10.2 Table 12 in the format specified by the SMETS1 Migration Schema embedded below.

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.

XML Element	Information
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. This shall contain one and only one of each of: • CriticalNetworkOperatorCertificateID • NonCriticalNetworkOperatorCertificateID • CriticalSupplierCertificateID • NonCriticalSupplierCertificateID
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. This shall contain one and only one of each of: • CriticalSupplierCertificateID • NonCriticalSupplierCertificateID 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

XML Element	Information
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 [[**TBC**]]
DeviceType	For the Device to which this element relates, the value required by DUIS in the [[**TBC**]]
DeviceModel	For the Device to which this element relates, the value required by DUIS in the [[**TBC**]]
DeviceManufacturer	For the Device to which this element relates, the value required by DUIS in the [[**TBC**]]
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.
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 Group ID for the set of SMETS1 Installations detailed in this file.
CriticalNetworkOperatorCertificate ID	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

XML Element	Information
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
S1SPEncryptedKey	As required by Clause 11.
EncryptedMasterKey	As required by Clause 11.
DecryptedS1SPGroupInformation	As required by Clause 11.
DecryptedMasterKey	As required by Clause 11.
S1SPGroupInformation	As required by Clause 11.
MasterKeyDetails	Either: • A structure containing one EncryptedMasterKey and a list of one of more DeviceIDs identifying which of the ESME, GPF and CHF the corresponding DecryptedMasterKey is the Master Key (with its DLMS COSEM meaning) for; or • A structure containing one EncryptedMasterKey and the DeviceID of the PPMID where the corresponding DecryptedMasterKey is the Master Key (with its DLMS COSEM meaning) for the PMMID.

<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 2 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 Section 3.10(b).

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>
</table>

Table 12

Schema be included once the content of this document is confirmed

10.3 Each file shall be named according to the following requirements (where || means concatenate):

FileType || RequesterID || MCFCounter || AdditionalID || ‘.xml’

where:

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

- FileType and AdditionalID have the values required by Table 13.

Type of file	FileType value	AdditionalID value	XML structure within file
Commissioning Outcome File	'COF'	COFCounter value from the file	CommissioningOutcomes
Migration Common File	'MCF'	Empty string	MigrationCommon
Migration Group File	'MGF'	MGFCounter value from the file	MigrationGroup
Migration Group Encrypted File	'MEF'	MEFCounter value from the file	MigrationGroupEncrypted
Migration Common Validation File	'MVF'	MVFCounter value from the file	MigrationValidation
S1SP Commissioning File	'SCF'	SCFCounter value from the file	S1SPOutcomes

Table 13

11 File Content Encryption and Decryption

11.1 A Requesting Party shall only have access to populated S1SPEncryptedKey, EncryptedMasterKey and S1SPGroupInformation elements 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 those elements.

11.2 When a SMETS1 SMSO generates a symmetric key for use in relation to this Clause 11, the DCC shall ensure that it shall generate a new such key for each S1SPGroupInformation it creates. The DCC shall ensure that the SMETS1 SMSO shall generate each such key using random numbers are such as to make it computationally infeasible to regenerate the key even with knowledge of when and by means of what equipment it were generated.

11.3 The DCC shall ensure that each SMETS1 SMSO shall, in populating the S1SPEncryptedKey and EncryptedMasterKey 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.

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

12 Requirements specific to GroupID = "AA" [DN: it is likely that three versions of this Appendix will be required for IOC, but the variants between them are catered for in this current generic version – some elements will need to be dis-applied for specific GroupIDs]

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

Pre-enrolment Configuration Requirements

12.2 Devices in the Group do not support any of the relevant functionality, and so none of the SMETS1 Supporting Requirements Clause 13 requirements lead to any actions being required to meet Pre-enrolment Configuration Requirements.

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 14 shall be the 'S1SP Migration Group 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

1	Confirm the following are present and populated validly within the entry with the CHFIdentifier for this SMETS1 Installation:
	• for the CHFDetails:
	  • SIMIdentifier [For Groups with SMS wake up]
	  • IPAddress [For Group with fixed internet protocol addresses on the CHF]
	  • PreviousAPN
	  [Note: select whichever of the above is required for this GroupID]

Table 14

DCO Migration Group Encrypted File data validation

12.7 The checks at **Error! Reference source not found.** 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
1	Confirm the following are present and populated validly for the entry with the CHFIdentifier for this SMETS1 Installation: • a MasterKeyDetails element which contains the DeviceID for each of the CHF, the GPF and the ESME • a MasterKeyDetails element which contains the DeviceID for each of the CHF and the GPF, and a MasterKeyDetails element which contains the DeviceID of the ESME • a MasterKeyDetails element which contains the DeviceID of the CHF, a MasterKeyDetails element which contains the DeviceID of the GPF and a MasterKeyDetails element which contains the DeviceID of the ESME
2	If the is a PPMIDIdentifier for this SMETS1 Installation in the Migration Common File, confirm the following are present and populated validly within the DecryptedGroupInformation for the entry with the CHFIdentifier for this SMETS1 Installation: • a MasterKeyDetails element which contains the DeviceID of the PPMID

Table 15

S1SP Migration Group Encrypted File data validation

12.8 The checks at Table 16 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

Step number	Check and processing

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
	  • PrepaymentWrapperKey
	  • PrepaymentWrapperWrapperKey

2	If the 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 • PrepaymentWrapperKey **[Note: delete where Group does not support it]** • PrepaymentWrapperWrapperKey **[Note: delete where Group does not support it]**

3	If the is a PPMIDIdentifier for this SMETS1 Installation in the Migration Common File, confirm the following are present and populated validly within the DecryptedS1SPGroupInformation for the entry with the CHFIdentifier for this SMETS1 Installation:
	• for the FirmwareAssociation:
	  • AuthenticationKey
	  • EncryptionKey

Table 16

S1SP / DCO Commissioning of SMETS1 Installation

12.9 The checks at Table 17 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		
1.X	The checks and processing required for 'Installing a SMETS1 Electricity Meter' for this Group ID, as specified in the SMETS1 Supporting Requirements, 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 the SMETS1 Supporting Requirements.
2.X	Where a GSMEDetail element is present, the checks and processing required for 'Installing a SMETS1 GSME' for this Group ID, as specified in the SMETS1 Supporting Requirements, shall be undertaken.	Yes	The error code for any failure that occurs, as defined in the SMETS1 Supporting Requirements.
3.X	Where a PPMIDDetail element is present, the checks and processing required for 'Installing a SMETS1 PPMID' for this Group ID, as specified in the SMETS1 Supporting Requirements, shall be undertaken.	Yes	The error code for any failure that occurs, as defined in the SMETS1 Supporting Requirements.

StepNumber	Check and processing	Critical?	SupportingData
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	
3.	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 1.	Yes	
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 1.	Yes	
5.X	For the CHF identified in the Migration Common File for this SMETS1 Installation, undertake the SMETS1 Supporting Requirements 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 the SMETS1 Supporting Requirements.

Table 17

12.10 The DCC shall develop and consult on a Commissioning 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 Commissioning Retry Strategy;

(c) the DCC shall publish a draft of the Commissioning 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.

12.11 Within 14 days of DCC publishing the draft Commissioning Retry Strategy pursuant to Clause 12.10 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 Commissioning Retry Strategy.

12.12 The Commissioning Retry Strategy may be updated following the procedure set out in Clause 12.10 and 12.11, provided that the DCC must ensure that

the most up to date Commissioning Retry Strategy is published to all Supplier Parties.

Installation Rollback

12.13 The processing at Table 18 shall be the 'Installation Rollback' for this GroupID**.**

Step number	Check and processing
1	The S1SP shall request that the DCO deletes 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 or raise an Incident if it cannot.
2	The S1SP shall deletes any keys and 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.
	The S1SP shall take reasonable steps to restore WAN communication between SMETS1 Installation and the relevant SMETS1 SMSO if possible.

Table 18

CHF Whitelist

12.14 The CHF Whitelist shall, for this Group IDs, 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.

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

[DN: the following sections to be placed in SMETS1 Supporting Requirements, since it applies equally to migrating Devices and those installed subsequently, as replacements for parts of migrated installations

13 Device installation – requirements specific to GroupID = "AA"

Installing a SMETS1 Electricity Meter

13.1 The following definitions shall be added to the SMETS1 Supporting Requirements:

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) 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) which the S1SP is required to use in relation to the Device's installation or Migration.

13.2 In this Clause 13.2, the term 'Application Association' shall have its GBCS meaning. 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.

13.3 The checks and processing at **Error! Reference source not found.** shall be that required of the S1SP and DCO for 'Installing a SMETS1 Electricity Meter' for this 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 which fail, checking and processing in relation to that SMETS1 Installation shall not proceed to a subsequent step.		
1	For each of the CHF, GPF 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.		
2	For each MasterKeyDetails for this SMETS1 Installation in the Authorised S1SP SMETS1 Device Credentials that relate to an ESME and / or CHF and / or GPF, request that the DCO validates and securely stores the DecryptedMasterKey and its association with the specified DeviceIDs.	Confirm that the MasterKeyDetails provided are semantically identical to the corresponding details in the Authorised DCO SMETS1 Device Credentials, then securely store the key (the 'Master Key') and its association to the DeviceIDs.	MasterKeyDetails
3	For each of the DataCollectionAssociation, ExtendedDataCollectionAssociation, ManagementAssociation and FirmwareAssociation within each of the CHFDetails, GPFDetails and ESMEDetails, request that the DCO validates and securely stores: • AuthenticationKey and its association to the DeviceID and 'name of Application Association', and • EncryptionKey and its association to the DeviceID and 'name of Application Association'	Confirm that the DCO has a securely stored Master Key for the DeviceID, and that it does not previously have a securely stored key of the 'key type' for this DeviceID. Where those checks succeed, the DCO shall securely store the key and its association with: • Its 'key type' • the 'name of Application Association' • the Device ID	DeviceID || 'name of Application Association' || 'key type' where: • 'key type' is one of 'AuthenticationKey' or 'EncryptionKey'; and • ''name of Application Association' is one of DataCollectionAssociation, ExtendedDataCollectionAssociation, ManagementAssociation or FirmwareAssociation
4	Using the AuthenticationKey and EncryptedKey in each of the DataCollectionAssociation, ManagementAssociation and FirmwareAssociation within each of the CHFDetails, GPFDetails 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.	**[DN: the change of keys for the ManagementAssociations and FirmwareAssociations will be a post commissioning obligation which will also be specified in the SMETS1 Supporting Requirements. It is that key change which will result in only the DCO having access to the associated Authentication Keys, and so only at that point will interactions with Devices require DCO interaction (and so allow DCO to cross check S1SP critical activities]**	DeviceID || 'name of Application Where 'name of Application Association' is one of DataCollectionAssociation, ExtendedDataCollectionAssociation, ManagementAssociation or FirmwareAssociation
5	Using the AuthenticationKey and EncryptedKey in the ExtendedDataCollectionAssociation in the CHFDetails: 1. confirm the successful creation of an Application Association with the Device, 2. read the CHF Whitelist, 3. close the Application Association 4. securely store each key and its association with: o Its 'key type' o the 'name of Application Association' o the Device ID		1, 2, 3 or 4 reflecting the sub step which failed
6	Using the AuthenticationKey and EncryptedKey in the ExtendedDataCollectionAssociation in the GPFDetails:		1, 2, 3 or 4 reflecting the sub step which failed

Error code on failure	S1SP checks and processing	DCO checks and processing	SupportingData
	1. confirm the successful creation of an Application Association with the Device, 2. read the Payment Mode (with its SMETS1 meaning), 3. close the Application Association 4. securely store each key and its association with: o Its 'key type' o the 'name of Application Association' o the Device ID		
7	Using the AuthenticationKey and EncryptedKey in the ExtendedDataCollectionAssociation in the ESMEDetails: 1. confirm the successful creation of an Application Association with the Device, 2. read the Payment Mode (with its SMETS1 meaning) 3. then close the Application Association 4. securely store each key and its association with: o Its 'key type' o the 'name of Application Association' o the Device ID If the Payment Mode is prepayment (with its SMETS1 meaning), using the AuthenticationKey and EncryptedKey in the ManagementAssociation in the ESMEDetails: 5. confirm the successful creation of an Application Association with the Device, 6. create and send a zero value 'Add Credit' instruction created using the PrepaymentKey in ESMEDetails, 7. confirm receipt of a successful response from the Device 8. close the Application Association 9. securely store the Prepayment Key and its association to the ESME Device ID		1, 2, 3, 4, 5, 6, 7, 8 or 9 reflecting the sub step which failed
8	For each MasterKeyDetails for this SMETS1 Installation in the Authorised S1SP SMETS1 Device Credentials that relate to an ESME and / or CHF and / or GPF: 1. Generate a new value for the AuthenticationKey and EncryptedKey for the DataCollectionAssociation for one of the Devices within MasterKeyDetails 2. Request that the DCO creates, using the relevant Master Key, the relevant form of the AuthenticationKey and EncryptedKey for inclusion in key change instructions to the Device 3. Request that the Device changes to use the new keys in this Application Association 4. Confirm that the Device has switched to using these new keys 5. securely store each new key and its association with: o Its 'key type' o the 'name of Application Association'	Create the relevant form of key required for inclusion in the instructions using the relevant Master Key. For clarity, the DCO does not exercise additional, independent controls on changes to keys in relation to Data Collection Application Associations, nor does it control access to such keys.	DeviceID, so identifying the Master Key which is not functioning

Error code on failure	S1SP checks and processing	DCO checks and processing	SupportingData
	○ the Device ID 6. invalidate the replaced keys		
9	Instruct the DCC to add the relevant CHF details to the Smart Metering Inventory.		

Table 19

13.4 The processing at **Error! Reference source not found.** 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 which fail, checking and processing in relation to that SMETS1 Installation shall not proceed to a subsequent step		
1	Using the DeviceID for the CHF on which the GSME should have been whitelisted: 1. Retrieve the AuthenticationKey and EncryptedKey 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
2	Using the Device ID of the GPF associated with the GSME 1. Retrieve the AuthenticationKey and EncryptedKey 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 Payment Mode (with its SMETS1 meaning) 4. then close the Application Association If the Payment Mode is prepayment (with its SMETS1 meaning), using the AuthenticationKey and EncryptedKey in the ManagementAssociation in the GSMEDetails: 5. confirm the successful creation of an Application Association with the Device, 6. create and send a zero value 'Add Credit' instruction created using the PrepaymentKey in GSMEDetails, 7. confirm receipt of a successful response from the Device 8. close the Application Association 9. securely store the PrepaymentKey and its association to the GSME Device ID		1, 2, 3, 4, 5, 6, 7, 8 or 9 reflecting the sub step which failed

Error code on failure	S1SP checks and processing	DCO checks and processing	SupportingData

Table 20

13.5 The processing at **Error! Reference source not found.** 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 which fail, checking and processing in relation to that SMETS1 Installation shall not proceed to a subsequent step		
	[TBC]		

Table 21