Version 2.~~0~~1

Appendix AS

ECoS Transition and Migration Approach Document

1 Introduction and General Obligations and Application of ETMAD

1.1 This Appendix is the ECoS Transition and Migration Approach Document (**ETMAD**).

1.2 Where directed to do so by the Secretary of State from time to time, the DCC shall develop and consult upon a further draft or drafts of this ETMAD and submit it to the Secretary of State in accordance with the process set out in Section G11.6 of the Code.

1.3 Subject to Clause 1.4 ~~and Clause 1.15~~, the DCC shall attempt ECoS Migration for all eligible TCoS Devices as soon as reasonably practicable. Devices shall only be eligible for ECoS Migration where they have been Commissioned (or in the case of a Gas Proxy Function has been installed as part of a Communications Hub Function that has been Commissioned) and have not subsequently been Decommissioned.

1.4 The DCC shall not attempt to migrate a particular Device that is deemed to be Ineligible for ECoS Migration. Devices may be Ineligible for ECoS Migration where:

(a) the Device is of a Device Model that has been classified as Non-Migratable;

(b) there is a transient issue which may impact the effectiveness of ECoS Migration such as recent or pending change of supplier, or recent Commissioning; or

(c) there is a technical issue impacting the functionality of the Device.

If the issue which made the Device Ineligible for ECoS Migration is subsequently resolved and / or no longer applies, the relevant Device shall no longer be Ineligible for ECoS Migration and the DCC shall attempt ECoS Migration for the Device in accordance with Clause 1.3.

1.5 The Responsible Supplier for each Device that holds Device Security Credentials that are populated from a TCoS Certificate, authorises the DCC to take the steps and carry out the processing set out in this ETMAD in order to ECoS Migrate each such Device.

1.6 The DCC shall not commence Bulk Migration for Devices of a particular Device Model until the DCC is reasonably satisfied that the DCC Systems can successfully migrate a Device of that particular Device Model in accordance with Clause 6.1(b).

1.7 Where the ECoS Migration of an individual Device is unsuccessful, the DCC shall complete remediation activities in accordance with the ECoS Migration Error Handling and Retry ~~Strategy~~Approach, as further described in Clause 7.

1.8 The DCC shall issue reports to Supplier Parties in accordance with the ECoS Migration Reporting Regime, as further described in Clause 4. As a minimum these reports will contain details of:

(a) Devices that have Failed Migration; and

(b) Device Models that are categorised as Non-Migratable, together with the DCC's supporting rationale.

1.9 Responsible Suppliers shall monitor reports provided in accordance with Clause 1.8 and shall endeavour to resolve issues which led to the Failed Migration of Devices for which they are the Responsible Supplier, in accordance with the ECoS Migration Error Handling and Retry ~~Strategy~~Approach.

1.10 Subject to Clause 1.11, where a Device is identified as being of a Device Model categorised as Non-Migratable or the issues leading to Failed Migrations cannot be resolved in accordance with Clause 1.9, the Responsible Supplier (except in the case of a Gas Proxy Function) shall upgrade the existing firmware version to a version of firmware that is functionally capable of ECoS Migration.

1.11 Where a Gas Proxy Function Device Model is identified as being of a Device Model categorised as Non-Migratable or the issues leading to Failed Migrations of a Gas Proxy Functions cannot be resolved in accordance with the ECoS Migration Error Handling and Retry ~~Strategy~~Approach, the DCC shall be responsible for completing remediation activities with the aim of enabling ECoS Migration to proceed, including upgrading the existing firmware version to a version of firmware that is functionally capable of ECoS Migration (where applicable).

1.12 The DCC shall publish a list of Non-Migratable Device Models ~~on the DCC~~

~~Website~~, to be updated regularly and as soon as practicable to reflect any changes identified.

1.13 Where a Party disagrees with the categorisation of a particular Device Model as Non-Migratable, the DCC shall endeavour to reach an agreed position with that Party. Where agreement cannot be reached, Parties may appeal the DCC's decision to categorise the Device Model as Non-Migratable to the Secretary of State.

1.14 Where an appeal has been made pursuant to Clause 1.13, the determination by the Secretary of State shall be final and binding for the purposes of this Code, provided that where a Device Model is categorised as Non-Migratable, the DCC may subsequently re-categorise the Device Model as being capable of ECoS Migration.

1.15 Supplier Parties shall manage their inventory of Devices to prioritise the installation and Commissioning of TCoS Devices ahead of ECoS Devices. Supplier Parties shall take all reasonable steps to ensure manufacturers update their processes to initiate production of ECoS Devices as soon as reasonably practicable following receipt of the ECoS Certificate from the DCC.~~Supplier Parties shall cease to install TCoS Devices thirty (30) days prior to the end of the ECoS Migration Period. In the event that TCoS Devices are installed after this date, there shall be no obligation on the DCC to perform or complete ECoS Migration in respect of such Devices~~.

1.16 The DCC shall manage the inventory ~~prioritise the provision~~ of Communications Hubs to prioritise the provision of those that include Gas Proxy Functions with TCoS Certificates ahead of those with ECoS Certificates. The DCC shall take all reasonable steps to ensure providers of Communication Services update their processes to initiate production of ECoS Devices as soon as reasonably practicable following receipt of the ECoS Certificate from the DCC.~~The DCC shall cease provision of Communications Hubs that include Gas Proxy Functions with TCoS Certificates 225 days following commencement of the ECoS Migration Period.~~

1.17 Prior to the addition of a new Device Model to the Certified Products List within the ECoS Migration Period, Supplier Parties intending to install Devices of that new Device Model shall ensure that, where reasonably practicable, testing is completed to demonstrate that ECoS Migration can be successfully performed on Devices of that Device Model, including the successful processing of a CoS Update Security

Credentials Service Request (Service Reference Variant 6.23) after ECoS Migration has taken place.

1.18 The DCC shall provide updates and reports from time to time, to the Secretary of State relating to activities carried out in accordance with this ETMAD, in a format and frequency to be mutually agreed between the DCC and the Secretary of State.

1.19 Prior to the end of the ECoS Migration Period, DCC shall ensure that the ECoS Party has the required information to enable processing of CoS Update Security Credentials Service Requests (Service Reference Variant 6.23) for all SMETS1 Devices.

1.20 The ECoS Party may commence processing of CoS Update Security Credentials Service Requests (Service Reference Variant 6.23) for SMETS1 Devices at any time within the ECoS Migration Period, provided that relevant testing has been completed in accordance with the ECoS Testing Approach Document.

1.21 For the purposes of Section G11.11 of the Code, this ETMAD shall no longer apply (and shall be automatically deleted from the Code) on 1 November 2024 (or any such later date as the Secretary of State may direct following consultation on a proposed alternative with the Parties and the Panel).

2 Defined Terms and Interpretation for the purposes of ETMAD

Bulk Migration	means the ECoS Migration of more than a defined number of Devices of a particular Device Model. The number of Devices which constitutes Bulk Migration for a particular Device Model shall be defined by the DCC. For the avoidance of doubt, until the proving activities set out in Clause 6.2(b) have been successfully completed, no more than three hundred (300) Devices of a particular Device Model shall be migrated.

ECoS Device	means a Device which has Device Security Credentials which pertain to the ECoS Party.
ECoS Migration	has the meaning given to that term in Section G11.12 of this Code and the term "**ECoS Migrate**" shall be interpreted accordingly.
ECoS Migration Error Handling and Retry ~~Strategy~~Approach	means the document defined in Clause 7.1.
ECoS Migration Incident	means an Incident that relates to the Services provided pursuant to this ETMAD.
ECoS Migration Period	means the period from commencement of ECoS Migration until this ETMAD is no longer applicable, in accordance with Clause 1.21.
ECoS Migration Reporting Regime	means the document defined in Clause 4.
ECoS Party	means the DCC when discharging the role of the ECoS Party.
Failed Migration	means in relation to a Device, the failure to complete any one or more of the steps specified in Clause 6.1(c).
Ineligible for ECoS Migration	means a status applied to a Device where DCC shall not attempt ECoS Migration as further described in Clause 1.4.
Non-Migratable	(in respect of Devices of a particular Device Model) means that the DCC considers it to be (i) technically or

	operationally impracticable, or (ii) disproportionately costly to attempt or re-attempt ECoS Migration. Such determination by the DCC shall be subject to any determination to the contrary by the Secretary of State in response to an appeal as set out in Clause 1.13.
TCoS Device	means a Device which has Device Security Credentials which pertain to the TCoS Party.

2.1 For the purposes of this ETMAD, where any reference is made (either directly or indirectly) to the Device Model of a Gas Proxy Function, this shall be interpreted as a reference to the Device Model of the Communications Hub of which that Gas Proxy Function forms part.

2.2 For the purposes of this ETMAD, where any reference is made (either directly or indirectly) to the Responsible Supplier of a Gas Proxy Function, this shall be interpreted as the Responsible Supplier for the Gas Smart Meter Equipment connected to the Communications Hub, where available. Where there is no Gas Smart Meter Equipment connected to the Communications Hub, the Responsible Supplier of the Gas Proxy Function, shall be interpreted as the Responsible Supplier for the Electricity Smart Meter Equipment connected to the Communications Hub, where available. Where there is neither any Gas Smart Meter Equipment nor any Electricity Smart Meter Equipment, there will be no Responsible Supplier.

3 Transitional Application of Sections of the Code

Application of Section A (Definitions and Interpretation)

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

(a) the definition of "DCC Individual Live Systems" (which has been replaced by the SMETS1 Transition and Migration Approach Document – Appendix AL) shall be amended to read as follows:

DCC Individual Live System

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

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

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

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

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

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

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

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

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

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

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

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

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

(b) the definition of "DCC Live Systems" (which has been replaced by the SMETS1 Transition and Migration Approach Document – Appendix AL) amended to read as follows:

DCC Live Systems means, with regard to the DCC's duty to Separate parts of the DCC Total System, those parts of the DCC Total System which are used for the purposes of:

(a) (other than to the extent to which the activities fall within paragraph (b), (c), (f), (g), (h), (i), (j), (k), (l) or (m) below) processing Service Requests, Pre-Commands, Commands, 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 (other than that carried out by a DCO, a SMETS1 Service Provider or the CoS Party) and (other than to the extent to which the activity falls within paragraph (d), (f), (g), (h), (i), (j), (k) or (l) below) Cryptographic Processing relating to the generation and use of

a Message Authentication Code and Countersigning SMETS1 Service Requests;

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

(d) providing SMKI Services;

(e) the Self-Service Interface;

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

(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 the CSS Provider in its capacity as such;

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

(l) discharging the obligations of the Commissioning Party in its capacity as such; and

(m) <u>discharging the obligations of the TCoS Party in its capacity as such,</u>

each of which shall be treated as an individual System within the DCC Live Systems.

(c) the definition of "Signed Pre-Command" shall be amended to read as follows:

Signed Pre-Command	means a communication containing the Digitally Signed GBCS Payload of a Pre-Command that has been Digitally Signed by a User, the CoS Party <u>or the TCoS Party.</u>

(d) the following definitions shall be added:

TCoS Party means the DCC when discharging the role of the TCoS Party.

TCoS Systems The DCC Systems that were used to support the operation of the CoS Party immediately prior to the commencement of ECoS Migration and that continue to be used to support the operation of the TCoS Party.

Application of Section G (Security)

3.2 Whilst this ETMAD remains in force, Section G (Security) of the Code shall be amended as follows:

(a) Clause G2.20(c) shall be replaced with the following:

'(c) subject to the provisions of Sections G2.21 and G2.22, each DCC Individual Live System is Separated from each other such System.'

(b) Clause G2.21 shall be replaced with the following:

'G2.21The DCC Individual Live System referred to at paragraph (m) of the definition of DCC Live Systems in Section A1 (Definitions) need not be Separated from the DCC Individual Live System referred to at paragraph (a) of that definition to the extent that it uses that System referred to at paragraph (a) solely for the purposes of confirming the relationship between:

(a) an MPAN or MPRN and any Party Details;

(b) an MPAN or MPRN and any Device; or

(c) any Party Details and any User ID.'

(c) Clause G2.44(a) amended such that the words "or TCoS Party" shall be added after the words "CoS Party".

(d) Clause G11.12 amended such that the words "and the ETMAD" shall be added after the words "For the purposes of this Section G11".

Application of Section H (DCC Services)

3.3 Whilst this ETMAD remains in force, Section H17.5 shall be amended to additionally include the following data items:

(a) ECoS party value;

(b) ECoS migration failure code;

(c) ECoS migration failure sub-code;

(d) ECoS migration date of last failure; and

(e) ECoS non-migratable flag.

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

~~3.3~~3.4 Whilst this ETMAD remains in force, Section L (Smart Metering Key Infrastructure and DCC Key Infrastructure) of the Code shall be amended as follows:

(a) In the table in Clause L3.18 the row corresponding to a Remote Party Role of 'transitionalCoS' shall be amended as follows:

transitionalCoS	The DCC	[Not applicable]	(c) or (m)

and the row corresponding to a Remote Party Role of 'coSPartyXmlSign' shall be amended as follows:

coSPartyXmlSign	The DCC	[Not Applicable]	(c) or (m)

(b) In the table in Clause L3.24 the row corresponding to a "DCC (transitionalCoS) Certificate" shall be amended as follows:

DCC (transitionalCoS) Certificate	digitalSignature	transitionalCoS	The role of the DCC as CoS Party or TCoS Party

Application of Appendix AB (Service Request Processing Document)

3.43.5 Whilst this ETMAD remains in force, Appendix AB (Service Request Processing Document) of the Code shall be amended as follows:

(a) Clause 6.4 shall be replaced with the following:

'6.4 Clause 6.5 shall apply subject to:

(a) (in relation to SMETS2+ Service Requests only) Clauses 9 (Obligations of the DCC: 'Request Handover of DCC Controlled Device' Service Requests), and 11 (User and DCC Obligations: 'Join Service' and 'Unjoin' Service Requests for Pre-Payment Meter Interface Devices and Gas Smart Meters);

(b) (for all Service Requests other than SMETS1 Service Requests targeted at a TCoS Device) Clause 8 (Obligations of the DCC: 'CoS Update Security Credentials' Service Requests and (where relevant) Corresponding Pre-Commands); and

(c) (for all Service Requests) Clause 18 (Obligations of the DCC: Non-Device Service Requests).'

(b) Clause 8 shall be replaced with the following:

'Obligations of the DCC: 'CoS Update Security Credentials' Service Requests and (where relevant) Corresponding Pre-Commands

8.1 The following shall apply in respect of each 'CoS Update Security Credentials' Service Request where the target Device of the Service Request is not a TCoS Device:

(a) where all of the requirements of Clause 6.1 are satisfied in respect of such a Service Request, the DCC shall send a Digitally Signed communication containing the 'CoS Update Security Credentials' Service Request (a "Countersigned CoS Service Request") to the CoS Party; and

(b) following receipt of the Countersigned CoS Service Request , and immediately prior to creating any corresponding Update Security Credentials Signed Pre-Command referred to in Clause 8.2, the CoS Party shall:

(i) Check Cryptographic Protection for the Countersigned CoS Service Request received;

(ii) Confirm Validity of the Certificates used to Check Cryptographic Protection;

(iii) apply the checks set out in Clauses 6.1(a), 6.1(d), 6.1(e.), 6.1(f), 6.1(g), 6.1(j) and 6.1(k) to the Service Request contained within the Countersigned CoS Service Request; and

(iv) confirm that the Service Request is not a Replay.

8.1A The following shall apply in respect of each 'CoS Update Security Credentials' Service Request where the target Device of the Service Request is a TCoS Device and the Service Request is not a SMETS1 Service Request:

(a) where all of the requirements of Clause 6.1 are satisfied in respect of such a Service Request, the DCC shall send a Digitally Signed communication containing the 'CoS Update Security Credentials' Service Request (a "Countersigned CoS Service Request") to the TCoS Party; and

(b) following receipt of the Countersigned CoS Service Request specified in Clause 8.1A(a), and immediately prior to creating any corresponding Update Security Credentials Signed Pre-Command referred to in Clause 8.2A, the TCoS Party shall:

(i) Check Cryptographic Protection for both the communication and for the Service Request included within it;

(ii) Confirm Validity of the Certificates used to Check Cryptographic Protection for both the communication and for the Service Request included within it;

(iii) confirm that User ID of the User who submitted the Service Request and the User ID contained within in each of the Organisation Certificates included within the Service Request are all associated with the same User; and

(iv) confirm that the User ID in each of the Organisation Certificates included within the Service Request is that of the Party who is identified via:

(A) the relevant MPRN or MPAN (as applicable) included within the Service Request; and

(B) the Registration Data for that relevant MPRN or MPAN,

as being the Party who is (or is to be) the Responsible Supplier for the relevant Device on the specified execution date or, if the execution date is not specified, on the current date.

8.2 Where, in respect of the communication received in relation to a 'CoS Update Security Credentials' Service Request, the requirements of Clause 8.1(b) are satisfied, the CoS Party shall apply CoS Party Threshold Anomaly Detection in accordance with the requirements of Clause 20 (CoS Party Threshold Anomaly Detection), which may result in a cessation of processing of the Service Request by the CoS Party, but otherwise either;

(a) where the target Device of the original 'Cos Update Security Credentials Service Request is a SMETS2+ Device,

(i) generate the GBCS Payload of an 'Update Security Credentials' Signed Pre-Command that is substantively identical to the 'CoS Update Security Credentials' Service Request;
(ii) Digitally Sign the GBCS Payload;
(iii) Incorporate the Digitally Signed GBCS Payload and the original Service Request into a single communication and Digitally Sign the communication with a CoS Party XML Signing Key to create a CoS Authorisation Response; and
(iv) send the signed CoS Authorisation Response to the DCC, or

(b) where the target Device of the original 'Cos Update Security Credentials Service Request is a SMETS1 Device:

(i) Digitally Sign the communication with a CoS Party XML Signing Key to create a CoS Authorisation Response; and

(ii) send the signed CoS Authorisation Response to the DCC.

8.2A Where, in respect of the communication received in relation to a 'CoS Update Security Credentials' Service Request, the requirements of Clause 8.1A (b) are satisfied, the TCoS Party shall:

(a) generate the GBCS Payload of an 'Update Security Credentials' Signed Pre-Command that is substantively identical to the 'CoS Update Security Credentials' Service Request;

(b) Digitally Sign the GBCS Payload; and

(c) send the resultant communication as a Signed Pre-Command to the DCC.

8.3 Where, in respect of a communication received in relation to a 'CoS Update Security Credentials' Service Request, the requirements of Clause 8.1(b) are not satisfied:

(a) the CoS Party shall not undertake any further processing of the communication, and shall notify the DCC; and

(b) the DCC shall notify the User that sent the original Service Request that the Service Request cannot be processed (such notification to be sent via the DCC User Interface).

8.3A Where, in respect of the communication received in relation to a 'CoS Update Security Credentials' Service Request, the requirements of Clause 8.1A (b) are not satisfied:

(a) the TCoS Party shall not undertake any further processing of the communication and shall notify the DCC; and

(b) the DCC shall notify the User that sent the original Service Request that the Service Request cannot be processed (such notification to be sent via the DCC User Interface).

8.4 Where the DCC receives a CoS Authorisation Response from the CoS Party, the DCC shall apply the following checks:

(a) Check Cryptographic Protection for the CoS Authorisation Response;

(b) Confirm Validity of the Certificates used to Check Cryptographic Protection for the CoS Authorisation Response;

(b) Confirm that the Remote Party Role of the Certificate used to Check Cryptographic Protection for the CoS Authorisation Response is 'coSPartyXmlSign'

(c) Confirm that the CoS Authorisation Response is valid and well formed;

(d) Confirm that the CoS Authorisation Response maps to a Countersigned CoS Service Request that was previously sent to the CoS Party;

(e) apply the checks set out in Clauses 6.1(a), 6.1(d), 6.1(e.), 6.1(f), 6.1(g), 6.1(j) and 6.1(k) to the Service Request contained within the CoS Authorisation Response;

(f) (in the circumstances where the target Device of the original 'CoS Update Security Credentials Service Request is a SMETS2+ Device only) confirm that the Signed Pre-Command contained within the CoS Authorisation Response is substantively identical to the Service Request contained within the CoS Authorisation Response; and

(g) confirm that neither the CoS Authorisation Response, nor the Service Request contained within it is a Replay.

8.4A Where the DCC receives a Signed Pre-Command from the TCoS Party, the DCC shall apply the following checks:

(a) confirm that the User ID within each Organisation Certificate within the Signed Pre-Command is the same as the User ID within the corresponding Organisation Certificate in the original 'CoS Update Security Credentials' Service Request;

(b) confirm that the Device ID within the Signed Pre-Command is the same as the Device ID included in the corresponding 'CoS Update Security Credentials' Service Request;

(c) confirm that the message originated from the TCoS Party by Checking the Cryptographic Protection for the message;

(d) Confirm Validity of the Certificates used to Check Cryptographic Protection for the message;

(e) Confirm Validity of all Certificates contained within the Signed Pre-Command; and

(f) confirm that the User ID in each of the Organisation Certificates included within the Signed Pre-Command is that of the Party who is identified via:

(i) the relevant MPRN or MPAN (as applicable) with which the Device specified in the Signed Pre-Command is associated in the Smart Metering Inventory; and
(ii) the Registration Data for that relevant MPRN or MPAN,

as being the Party who is (or is to be) the Responsible Supplier for the relevant Device on the specified execution date or, if the execution date is not specified, on the current date.

8.5 Subject to Clause 14 (Orchestration of Service Requests), where all of the requirements of Clause 8.4 are satisfied in respect of a CoS Authorisation Response received from the CoS Party, the DCC shall:

(a) (in the circumstances where the target Device of the original ‘CoS Update Security Credentials Service Request is a SMETS2+ Device) send a Command associated with the Signed Pre-Command contained within the CoS Authorisation Response in accordance with Clause 13 (DCC Obligations: Sending Commands); or

(b) (in the circumstances where the target Device of the original ‘CoS Update Security Credentials Service Request is a SMETS1 Device) Countersign the CoS Update Security Credentials Service Request and send the Countersigned Service Request to the relevant SMETS1 Service Provider in accordance with the requirements of Clause 14.

8.5A Subject to Clause 14 (Orchestration of Service Requests), where all of the requirements of Clause 8.4A are satisfied in respect of a Signed Pre-Command received from the TCoS Party, the DCC shall send the associated Command in accordance with Clause 13 (DCC Obligations: Sending Commands).

8.6 Where any of the checks in Clause 8.4 are not satisfied in respect of a CoS Authorisation Response received from the CoS Party, the DCC shall:

(a) not be obliged to undertake any of the other checks that remain to be undertaken, and the DCC shall reject the CoS Authorisation Response;

(b) save where Clause 8.4(c) is not satisfied, notify the CoS Party of such rejection and of the reasons for such rejection; and

(c) notify the User that sent the original 'CoS Update Security Credentials' Service Request.

8.6A Where any of the checks in Clause 8.4A are not satisfied in respect of a Signed Pre-Command received from the TCoS Party, the DCC shall: not be obliged to undertake any of the other checks that remain to be undertaken, and the DCC shall reject the Signed Pre-Command;

(a) save where Clause 8.4A(c) is not satisfied, notify the TCoS Party of such rejection and of the reasons for such rejection; and

(b) notify the User that sent the original 'CoS Update Security Credentials' Service Request.'

Application of Appendix AC (Enrolment, Inventory and Decommissioning Procedures)

~~3.5~~3.6 Whilst this ETMAD remains in force, Appendix AC (Enrolment, Inventory and Decommissioning Procedures) of the Code shall be amended as follows:

a) Clause 5.19 shall not apply; and

b) the text immediately below the table in Clause 3.2 shall be replaced with the following:

Where 'DCC Recovery Certificate', 'DCC CoS Certificate', 'DCC Access Control Broker Certificate' and 'DCC WAN Provider Certificate' are each Organisation Certificates created by the DCC for the purposes of occupying the relevant Trust Anchor Cells on Devices in accordance with the above table and used by those DCC Systems described in (respectively) sub-paragraphs (f), (c) or (m), (b) and (a) of the definition of DCC Live Systems.

Application of Appendix AG (Incident Management Policy)

~~3.6~~3.7 Whilst this ETMAD remains in force, Appendix AG (Incident Management Policy) of the Code shall be amended as follows:

(a) the definition of Live Services (which has been replaced by the SMETS1 Transition and Migration Approach Document – Appendix AL) shall be replaced as follows:

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

(b) Clause 2.1.3 shall not apply in respect to ECoS Migration Incidents;

(c) Clause 5.2 shall not apply in respect of DCC Systems to the extent that they are being used for ECoS Migration;

(d) where the DCC ought to be reasonably able to resolve an ECoS Migration Incident without the assistance of any Responsible Supplier, any incident resolution activities associated with an ECoS Migration Incident shall be assigned to the DCC; otherwise the incident resolution activities shall be assigned to the Responsible Supplier;

(e) the DCC shall raise an ECoS Migration Incident where monitoring of the DCC Systems identifies a problem with the DCC Systems to the extent that they are being used for ECoS Migration.

(f) the DCC shall not be required to raise an Incident, and no Party shall have the right to raise an ECoS Migration Incident, in circumstances where a Responsible Supplier is notified by the DCC in accordance with this ETMAD that one or more of the steps in the ECoS Migration of an individual Device has not been

successfully completed, unless this is required by the ECoS Migration Error Handling and Retry ~~Strategy~~Approach;

(g) Table 1 in Clause 2.4 shall be amended to include the following descriptions:

- Category 1 Incident: has a critical adverse impact on the activities necessary to carry out ECoS Migration pursuant to the ECoS Transition and Migration Approach Document;
- Category 2 Incident: has a non-critical adverse impact on the activities necessary to carry out ECoS Migration pursuant to the ECoS Transition and Migration Approach Document;
- Category 3 Incident: has a moderate adverse impact on the activities necessary to carry out ECoS Migration pursuant to the ECoS Transition and Migration Approach Document;
- Category 4 Incident: has a minor adverse impact on the activities necessary to carry out ECoS Migration pursuant to the ECoS Transition and Migration Approach Document;
- Category 5 Incident: has a minimal adverse impact on the activities necessary to carry out ECoS Migration pursuant to the ECoS Transition and Migration Approach Document; and

(h) Table 3 in Clause 5.2.1, row D8, column 2 shall be amended as follows: "The DCC experiences a failure of the systems used to support the operation of the CoS Party or TCoS Party".

Application of Section M (General)

~~3.7~~3.8 The Responsible Supplier for each Device referred to in Clause 1.3 acknowledges that the carrying out of one or more of the steps referred to in this ETMAD, 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. The DCC shall not be liable to the Responsible Supplier (or any other Party) for any Liability that arises from the carrying out of (or attempt to carry out) any of those steps, where (and to the extent

that) the DCC has acted in accordance with this ETMAD.

~~3.8~~3.9 The DCC shall carry out the activities and provide the services described in this ETMAD in accordance with Good Industry Practice. Each Responsible Supplier shall act in accordance with Good Industry Practice when providing support or assistance and carrying out remediation activities referred to in this ETMAD, in particular as set out in Clause 1.9.

~~3.9~~3.10 (Save for in respect of the Gas Proxy Function Device Model as set out in Clause 1.11 or where explicitly provided in this ETMAD) the DCC shall have no obligation or liability in respect of the ECoS Migration of any Device which is deemed to be Ineligible for ECoS Migration until or unless the issue which made the Device Ineligible for ECoS Migration is subsequently resolved and / or no longer applies, such that the Device is no longer Ineligible for ECoS Migration. For avoidance of doubt, the DCC shall have no obligation or liability in respect of the ECoS Migration of any Device with a Device Model that is categorised as Non-Migratable).

4 Reporting

4.1 The DCC shall make available to the Panel, all Parties and (on request) the Secretary of State the ECoS Migration Reporting Regime that includes a list of the reports that the DCC shall provide to Supplier Parties in respect of ECoS Migration and provides an overview of the frequency, content of and recipients of those reports.

Updating the ECoS Migration Reporting Regime

4.2 Except where the modification to the ECoS Migration Reporting Regime is of a minor typographical nature or where the modification has no material effect on the rights or obligations of Parties, any updates to the ECoS Migration Reporting Regime shall be made according to the following the procedure:

(a) the DCC shall produce and publish an initial draft of the revised ECoS Migration Reporting Regime for consultation with Supplier Parties and such other persons as are likely to be interested;

(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 Supplier Party in accordance with this Clause 4.

(c) the DCC shall publish an updated draft of the ECoS Migration Reporting Regime 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 updated 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 that have not been resolved by reaching an agreed proposal.

4.3 Within fourteen (14) days of DCC publishing the updated draft ECoS Migration Reporting Regime pursuant to Clause 04.2(c), 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 updated draft published by the DCC shall become the agreed ECoS Migration Reporting Regime at the expiry of the fourteen (14) day period following its publication.

4.4 Where the modification to the ECoS Migration Reporting Regime is of a minor typographical nature or where the modification has no material effect on the rights or obligations of Parties, the DCC shall make the revised ECoS Migration Reporting Regime available to all Supplier Parties ~~by publishing it on the DCC Website~~ including providing the date on which it intends that the updated ECoS Migration Reporting Regime shall come into effect.

4.5 For each Supplier Party, the DCC shall detail directory structures in DCC's secure document management and storage system through which that Supplier Party can access its reports. The DCC shall provide a Supplier Party with only those files which are relevant to that Supplier Party and the DCC shall do so through the secure document management and storage system (which, at the time of drafting of this ETMAD is DCC's Microsoft SharePoint).

5 Provision of Information to the DCC

5.1 Each Supplier Party shall, on request from the DCC and within such reasonable time period as the DCC may specify, provide such information as may be reasonably required by the DCC to enable it to plan, co-ordinate, and undertake (and provide ongoing support for) ECoS Migration.

6 Migration Approach

6.1 The DCC shall determine:

(a) the process for selecting Devices for ECoS Migration, taking into account the Device Models and any exclusions as set out in Clause 1.4;

(b) the process for initiating ECoS Migration in a controlled and managed way, on the basis that, as a minimum, the DCC shall not commence Bulk Migration for Devices of a particular Device Model until it has first:

(i) successfully replaced the TCoS Certificate with an ECoS Certificate or a different TCoS Certificate on; and

(ii) subsequently demonstrated that a CoS Update Security Credentials Service Request (Service Reference Variant 6.23) has been successfully processed by,

a Device of that Device Model or a Device Model to which it can be upgraded by a firmware upgrade as set out in more detail in Clause 6.2, where activities referenced in 6.1(b)(i) and (ii) may have occurred prior to this version of the ETMAD becoming effective;

(c) the steps required to successfully complete ECoS Migration for an individual Device, including:

(i) the instruction to the TCoS Service Provider to initiate ECoS Migration;

(ii) review by the TCoS Service Provider to confirm that ECoS Migration can commence;

(iii) replacement of the Device Security Credentials that pertain to the TCoS

Party with those that pertain to the ECoS Party on the relevant Device; and

(iv) confirmation received from both the ECoS Service Provider and TCoS Service Provider that ECoS Migration has completed successfully.

(d) the process for managing Failed Migrations, including the suspension of ECoS Migration for certain Device Models to allow issues to be investigated and prevent ECoS Migration of Devices categorised as Non-Migratable; and

(e) the process for determining whether a Device Model should be categorised as Non-Migratable, subject to Clause 1.14.

6.2 For avoidance of doubt, Clause 6.1(b) allows DCC to commence Bulk Migration of Devices of a particular Device Model where the requirements set out at Clause 6.1(b)(i) and (ii) have been met for at least one Device of either (a) the same Device Model or (b) a Device Model with the same Manufacturer, same model and same hardware version but with a later firmware version, on the basis that, if ECoS Migration fails for any such Devices, the firmware version can be upgraded to a firmware version capable of ECoS Migration.

7 Error Handling and Retry ~~Strategy~~Approach

7.1 The DCC shall make available to the Panel, all Parties and (on request) the Secretary of State the ECoS Migration Error Handling and Retry ~~Strategy~~ Approach that details the activities the DCC shall carry out where an ECoS Migration attempt is unsuccessful and the resolution activities the Supplier Party shall carry out in relation to Failed Migrations.

Updating the ECoS Migration Error Handling and Retry ~~Strategy~~Approach

7.2 Except where the modification to the ECoS Migration Error Handling and Retry ~~Strategy~~ Approach is of a minor typographical nature or where the modification has no material effect on the rights or obligations of Parties, any updates to the ECoS Migration Error Handling and Retry ~~Strategy~~ Approach shall be made according to the following the procedure:

(a) the DCC shall produce and publish an initial draft of the revised ECoS Migration

Error Handling and Retry ~~Strategy~~ Approach for consultation with Supplier Parties and such other persons as are likely to be interested;

(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 Supplier Party in accordance with this Clause 7.

(c) The DCC shall publish an updated draft of the ECoS Migration Error Handling and Retry ~~Strategy~~ Approach 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 updated 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 that have not been resolved by reaching an agreed proposal.

7.3 Within fourteen (14) days of DCC publishing the updated draft ECoS Migration Error Handling and Retry ~~Strategy~~ Approach pursuant to Clause 0~~7.2~~(c), 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 updated draft published by the DCC shall become the agreed ECoS Migration Error Handling and Retry ~~Strategy~~ Approach at the expiry of the fourteen (14) day period following its publication.

7.4 Where the modification to the ECoS Migration Error Handling and Retry ~~Strategy~~ Approach is of a minor typographical nature or where the modification has no material effect on the rights or obligations of Parties, the DCC shall make the revised ECoS Migration Error Handling and Retry ~~Strategy~~ Approach available to all Supplier Parties ~~by publishing it on the DCC Website~~ including providing the date on which it intends that the updated Migration Error Handling and Retry ~~Strategy~~ Approach shall come into effect.