Data Communications Company

Consultation

On the "Go Live" version of the ECoS Transition and Migration Approach Document (ETMAD) – SEC Appendix AS

Date: 11.04.2022
Classification: DCC Public

Table of Contents

1. Introduction

1.1. Purpose of this consultation

1. This consultation seeks stakeholder views on the proposed drafting for the revised version of the ECoS Transition and Migration Approach Document (ETMAD) that needs to be re-designated to take effect and be re-incorporated into the Smart Energy Code (SEC), at the Enduring Change of Supplier (ECoS) Service Live Date, referred to as the "Go Live ETMAD".

2. The initial version of the ETMAD was introduced into the SEC on 25 October 2021, at the time when the SEC main body changes required for ECoS also came into effect. The primary purpose of this initial version of the ETMAD is essentially to undo the ECoS related main body SEC changes until the ECoS Migration commences. The Go Live ETMAD defines DCC and Supplier Party rights and obligations that are to be in place during the ECoS Migration Period. This includes changes to SEC provisions applicable during the transition from Transitional Change of Supplier (TCoS) to ECoS arrangements.

3. This ETMAD consultation overview document summarises and seeks stakeholder feedback on the proposed Go Live ETMAD attached to this consultation. After considering the feedback received via this ETMAD consultation, and any further discussion or consultation that may deemed to be required, changes to the ETMAD will be re-designated by the Department of Business, Energy and Industrial Strategy (BEIS) using powers under Condition 22 of the DCC Licence and Section X5 of the SEC at the time of ECoS Go Live – i.e. when migration of Devices from the TCoS Party to the ECoS Party can commence. This re-designation will be accompanied by the redesignation of the go-live versions of the other subsidiary documents which need to be modified on the ECoS Service Live Date and upon which the DCC consulted on 24 September 2021 and concluded on 9 February 2022.

4. In parallel with this consultation, DCC will continue engagement with industry via monthly drop-in sessions. Questions raised through these meetings have been collated into a set of 'Frequently Asked Questions' which DCC can make available on request.

5. The closing date for this ETMAD consultation is 12 May 2022.

1.2. Background and context

6. The ECoS arrangements are changes to the process that DCC follows when a consumer changes Supplier Party and the new Supplier Party seeks to take over control of the Smart Meter and other Devices in the consumer premises.

7. When a gas or electricity consumer with a Smart Meter switches Supplier Party, the security information held on the Smart Meter needs to be changed so that it relates to the new Supplier Party and not the old one. The processes that are currently in place for managing the change of security information held on Smart Meters are referred to as the TCoS processes and they are administered by part of the DCC Systems known as the "Change of Supplier Party" (CoS Party).

8. As their name suggests, the existing TCoS processes were intended to be temporary. Changes to replace the existing TCoS arrangements to the enduring solution are already underway. Following a direction issued by the Secretary of State under condition 13A of the DCC licence, on 1 August 2019 the DCC published a consultation on its draft plan for its delivery of the ECoS arrangements.

9. In 2021, DCC undertook a replanning exercise, resulting in changes to the ECoS Joint Industry Plan (JIP) milestones being issued for consultation in January 2022. Feedback was received from Implementation Managers Forum (IMF) and an ad hoc IMF meeting was held on 16 February for DCC to respond to this feedback. The outcome from this replanning exercise and subsequent

consultation was a revised set of JIP milestones, including an ECoS Service Live Date of 30 June 2023. Final approval for new ECoS JIP milestones was provided by the Smart Metering Delivery Group on 10 March 2022.

Development of SEC provisions

10. The introduction of the ECoS arrangements requires changes to the SEC main body as well as to several SEC Subsidiary Documents. BEIS published a consultation document on changes to the SEC main body required for the ECoS arrangements on 1 April 2021. The BEIS response to its consultation was published on 15 June 2021[1].

11. As outlined above, the SEC main body changes and the initial version of the ETMAD came into effect on 25 October 2021.

12. Additionally, DCC recently concluded a consultation on the SEC Subsidiary Document changes required for the ECoS arrangements. This covered changes to a number of SEC appendices including the Service Request Processing Document, Threshold Anomaly Detection Document, DCC User Interface Specification and the Inventory Enrolment and Decommission Procedures. This consultation ran from 24 September 2021 to 5 November 2021 and DCC published its conclusions document on 9 February 2022[2].

13. Within the conclusions document, DCC outlined that it has been developing a Go Live version of the ETMAD to be re-designated to take effect at the commencement of the ECoS Migration, alongside the changes to the other SEC Subsidiary Documents outlined in that consultation. The Go Live version of the ETMAD is planned to be used to control the process of transition and migration to ECoS and will:

    a) cease the suspension of the ECoS main body changes that have been introduced into the SEC;

    b) set out the arrangements whereby CoS Update Security Credentials Service Requests (SRV 6.23) are processed differently by DCC depending on whether the target Device holds Device Security Credentials that are ECoS related or TCoS related; and

    c) deal with other migration related matters.

14. The re-designation of SEC Subsidiary Documents to support the new ECoS arrangements (including the Go Live ETMAD) is due to take place at the new ECos Service Live Date of 30 June 2023, which marks the point at which TCoS to ECoS migration can legally commence.

15. In parallel with this ETMAD consultation, DCC is continuing work to develop further documentation to support ECoS Migration. The ECoS Migration Reporting Regime (EMRR) and ECoS Migration Error Handling and Retry Strategy (EMEHRS) which are explained further in sections 1.6 and 1.9 of this ETMAD consultation document will be subject to a separate industry consultation at a later date.

2. Contents of the “Go Live ETMAD”

16. To support respondents’ review of the proposed ETMAD drafting, we have summarised below, the key sections of the ETMAD and DCC’s considerations.

[1] https://smartenergycodecompany.co.uk/latest-news/beis-consultation-response-on-changes-to-the-sec-for-the-ecos-and-certain-security-provisions-and-direction-to-re-designate-the-smki-interface-design-specification/
[2] https://www.smartdcc.co.uk/consultations/conclusions-on-the-sec-subsidiary-document-changes-required-for-the-enduring-change-of-supplier-ecos-arrangements-and-consultation-on-date-for-re-designation-of-certain-documents/

1.3. Introduction and General Obligations

17. Section 1 of the ETMAD defines the obligations on DCC relating to the overall delivery of ECoS Migration throughout the ECoS Migration Period and also the obligations on Supplier Parties to manage their inventories of TCoS Devices and take appropriate actions where issues arise, which prevent one or more Devices from being migrated.

DCC Obligations

18. DCC's core obligation is to migrate all Devices within the ECoS Migration Period. The term 'Devices' covers all types of Device, including the Gas Proxy Function (GPF) which forms part of the Communications Hub. DCC will only attempt ECoS Migration where the Device has been commissioned. The exception to this is the GPF, which may be migrated if the associated Communications Hub Function has been commissioned, and the GPF has a SMI Status of either 'commissioned' or 'installed not commissioned', and therefore a caveat has been included to explain this nuance. This will prevent a scenario where DCC carries out ECoS Migration on an electricity only installation, leaving the Gas Proxy Function with a TCoS Certificate that would need migrating if a gas Device is installed and commissioned at a later date.

19. Two specific exclusions have been defined to reflect the fact that there will be circumstances where DCC knows in advance that ECoS Migration on certain Devices will not be successful. In these scenarios, DCC will not attempt ECoS Migration. These exclusions include fundamental issues impacting a whole Device Model (which defines the combination of model, manufacturer and firmware version) and Device specific issues, as set out below:

    a) Non-Migratable Device Models: DCC will carry out proving activities using a subset of Devices for each Device Model before initiating Bulk Migration. Where issues are encountered relating to a specific Device Model that lead to a Failed Migration, DCC may determine that the Device Model should be classed as Non-Migratable. No further attempts to migrate Devices of this Device Model will be made. Details of Non-Migratable Device Models will be provided to the Responsible Supplier via individual reports and a list on Non-Migratable Device Models will also be published on the DCC website for wider visibility to other market participants, including Meter Asset Providers (MAPs). Where a Supplier Party disagrees with the categorisation of a Device Model as Non-Migratable, they can appeal to the Secretary of State, whose determination will be final and binding.

    The expectation is that the number of Device Models categorised as Non-Migratable will be low and should be resolvable by a firmware upgrade. DCC is already carrying out TCoS to TCoS certificate transfers and evidence from these activities will feed into the determination of Device Models as Non-Migratable. Further information regarding this 'proving' process will be provided as more Device Models are tested.

    b) Ineligible Devices: Individual Devices will be excluded from selection for ECoS Migration where certain conditions apply. At a high level, Devices will be classified as ineligible where the associated Device Model is classified as Non-Migratable (as is outlined above); where there is a transient issue impacting the Device, for example recent commissioning or change of supplier has been undertaken; or where there is a technical issue with the Device, such as communications not working or inability to identify whether a TCoS or ECoS Certificate is held on the Device. If the issue that caused the Device to be ineligible for ECoS Migration no longer applies, for example where a Device of a Non-Migratable Device Model undergoes a firmware upgrade or the communications issue is resolved, DCC will attempt ECoS Migration in line with the selection process (as further described in Section 1.8 of this ETMAD consultation document).

20. In addition, DCC may determine whether to carry out further attempts of ECoS Migration for Devices where initial attempts have failed. The approach to handling errors, including the

number of attempts and re-tries will be set out in the ECoS Migration Error Handling and Retry Strategy, as further described in section 1.9 of this consultation document.

21. DCC's other key requirement is to provide information on the progress of ECoS Migration. This will take the form of progress updates and reporting to the Secretary of State and defined reports provided to Supplier Parties, as further described in section 1.6 of this consultation document. The reason for DCC issuing reporting to Supplier Parties is to update them with the detail and DCC's reasoning where ECoS Migration has failed, or Devices are categorised as Non-Migratable. The intention is that this will help those Supplier Parties resolve issues. DCC will consult on the specifics of the reporting regime for the ECoS Migration Period, separately to this ETMAD consultation.

Supplier Party Obligations

22. Supplier Party obligations are focused on resolution of ECoS Migration issues identified through DCC reporting. The ECoS Migration Error Handling and Retry Strategy will define the different types of error that may arise and the proposed remediation approach to be delivered by DCC and / or Supplier Parties.

23. Other than for GPFs which form part of the Communications Hub, where Devices of a particular Device Model are categorised as Non-Migratable, Supplier Parties will be responsible for upgrading the firmware to a version that is capable of ECoS Migration. This obligation is placed on the Responsible Supplier for each Device who has the supply licence obligation to take all reasonable steps to ensure that the Smart Metering System at the relevant premises is maintained, so that at all times it satisfies the requirements in the relevant Technical Specification. Similarly, where Supplier Parties are unable to resolve ECoS Migration issues in relation to individual Devices, then they may be required to upgrade the firmware version.

24. DCC is having ongoing discussions with BEIS regarding the inclusion of a requirement on Supplier Parties to replace Devices where the issue preventing ECoS Migration cannot be resolved via a firmware upgrade. DCC acknowledges concerns, raised by Supplier Parties and MAPs, that this may result in premature replacement of Devices that are otherwise fit for purpose. We have therefore been considering an alternative option to mitigate the risk that Devices will be stranded with TCoS Certificates at the point the TCoS Party is de-commissioned. This option would require the transfer of the TCoS private keys to the ECoS Party, enabling the ECoS Party to process SRV6.23s relating to TCoS Devices. In assessing this option, we are considering both the cost impact of this transfer and any associated security risks that this may introduce. To support this ongoing assessment, we are seeking views from respondents on the option, with responses feeding into the wider business case analysis which we are expecting to conclude by Autumn 2022. Further changes to the ETMAD may be required, depending on the outcome of this analysis. Any such changes will be subject to industry consultation at a later date.

25. Whilst the Responsible Supplier will have the obligation to carry out remediation activities, the ETMAD recognises the role of DCC in the provision of Communications Hubs. A specific carve out has been included relating to Gas Proxy Functions which cannot be migrated. In this scenario DCC may be required to deliver firmware updates where a Gas Proxy Function Device Model is categorised as Non-Migratable.

SMETS1 Devices

26. Most provisions within the ETMAD relate to SMETS2+ Devices as SMETS1 Devices do not contain DCC CoS Certificates and are therefore excluded from ECoS Migration. However, the ECoS Party will require information on SMETS1 Devices to correctly process SRV 6.23s. i.e. to refer these service requests to the relevant SMETS1 Service Provider.

27. DCC will be responsible for determining when data is passed to the ECoS Party, for example whether a single 'big bang' approach is followed, or a staggered approach throughout the ECoS

Migration Period. The ETMAD therefore recognises the need for the transfer of information without specifying the overall approach.

ECoS Migration Period

28. Based on the replanning exercise carried out in 2021, the ECoS Service Live Date is expected to be 30 June 2023. This reflects the start of the ECoS Migration Period covered by the ETMAD. As set out within the revised Joint Industry Plan, we expect ECoS Migration to conclude in April 2024 with DCC no longer relying on the provision of TCoS services under the TCoS Service Provider contract later that year. The ETMAD reflects this position by including 31 October 2024 as the date by which the ETMAD will no longer apply, with flexibility for this to be extended by the Secretary of State.

29. In defining the end of the ECoS Migration Period, we have acknowledged that discussions are ongoing between DCC and Supplier Parties to understand the numbers of TCoS Devices held in stock, to feed into the wider migration planning, for example the timing required for the provision of ECoS Certificates to enable manufacturers to initiate development of ECoS Devices ahead of ECoS Go Live. This will help DCC and BEIS assess the feasibility of the proposed timescales, avoiding the position where large numbers of TCoS Devices remain uninstalled at the end of the ECoS Migration Period. As part of these considerations, we are again discussing the alternative option highlighted above, where the TCoS private keys are transferred to the ECoS Party.

30. Therefore, rather than defining the end of the ECoS Migration Period as April 2024, to reflect the point that DCC plans to complete the majority of ECoS Migration, we have linked the end of the ECoS Migration Period to the 31 October 2024 date, at which point the ETMAD will cease to exist. This provides additional time for Supplier Parties to install TCoS Devices held in their inventory, with a clear obligation that requires Supplier Parties to prioritise the installation of TCoS Devices and cease installation 30 days before the end of the ECoS Migration Period i.e. by the end of September 2024. The final month is then available for DCC to migrate TCoS Devices installed in the latter months.

31. A complementary requirement has also been included for DCC to cease provision of Communications Hubs including Gas Proxy Functions with TCoS Certificates 225 days following commencement of the ECoS Migration Period. This timeline is subject to ongoing commercial discussions between DCC and its service providers.

32. The proposed ETMAD drafting provided alongside this consultation document is based on the assumption that a hard stop will be applied at the point the TCoS Party is de-commissioned, beyond which TCoS Devices will not be capable of switching Supplier Party. Should the ongoing discussions result in a decision to transfer TCoS private keys to the ECoS Party, revised drafting will be included within the ETMAD to reflect this position, which will be subject to a further consultation.

1.4. Definitions

33. Section 2 of the ETMAD includes a table of new definitions required to support the ECoS Migration, for the period that the ETMAD is in existence.

1.5. Transitional Application of Sections of the Code

34. Section 3 of the ETMAD includes cross references to a number of clauses within the SEC main body and appendices that require revision for the period the ETMAD is in place. Drafting within this section is based on the SEC text to be designated by BEIS in parallel with the ECoS Service Live Date (as issued for consultation in September 2021 and the subsequent conclusions document published in February 2022). This also takes into account the proposed drafting for the Central Switching Service modification, which introduces the CSS Provider within the definition of DCC Live Systems.

35. At the ECoS Service Live Date, the ECoS Party will become the CoS Party as referenced within the SEC. During the ECoS Migration Period, both the TCoS Party and the ECoS Party will be effective. Therefore, a number of clauses have been identified which will need to reference the TCoS Party in addition to the CoS Party, to reflect this parallel running. This includes definitions in Section A and references to the DCC CoS Certificate in Section L. The rationale for this, and other, changes introduced through Section 3 of the ETMAD is included in the tables below:

SEC Clause	ETMAD Approach
Clause A	The ETMAD introduces references to the TCoS Party within the definitions of DCC Live Systems, DCC Individual Live Systems and Signed Pre-Command. It also introduces new definitions of TCoS Party and TCoS Systems required for the ECoS Migration Period.
Clause G	One of the key principles behind the introduction of the ECoS Party was to enable separation of systems between the organisation processing CoS Security Credential updates and the rest of DCC Individual Live Systems. Prior to the designation of ECoS related changes to SEC drafting, Clause G2.21 enabled the existing CoS Party (i.e. the TCoS Party) to share registration data with the main DSP systems. This clause was removed by the changes designated on 25 October 21 and has been re-inserted through the initial ETMAD. Drafting within the existing ETMAD shall therefore be retained for the Go Live ETMAD to reflect the ongoing inclusion of the TCoS arrangements for the period of migration covered by the ETMAD.
Clause L	Minor changes to Clause L have been made to reference both the CoS Party and TCoS Party.
Clause M	Similar to clauses reflected in the SMETS1 TMAD (SEC Appendix AL), clauses have been added to the ETMAD to provide clarity that the Responsible Supplier and DCC will not be liable where migration or associated remediation activities have been delivered in accordance with Good Industry Practice. No additional limitation on liability has been added in relation to ECoS Migration activities and therefore existing limitations apply as set out in section M, which limit DCC's liability to £1m for each incident or series of incidents, which may arise.
Appendix AB	Two specific clauses in Appendix AB, the Service Request Processing Document (SRPD), are referenced within the ETMAD. Clause 6.4 is amended to clarify the routing of CoS Service Requests for both TCoS Devices and ECoS Devices. Clause 8 has been re-drafted in its entirety to reflect the parallel processing of CoS Service Requests by the TCoS Party and the ECoS Party.

	Note that there are no changes to the Threshold Anomaly Detection clauses as this is applied to ECoS and not TCoS, so no parallel running.
Appendix AC	A new alert to notify Supplier Parties where a device is being installed with a TCoS Certificate is being introduced into Appendix AC, to be designated by BEIS at ECoS Go Live. The ETMAD effectively switches this off during the ECoS Migration Period, while TCoS Devices are still being installed.
Appendix AG	The changes proposed to Appendix AG introduce a new category of incident, ECoS Migration Incident. Changes include reference to ECoS Migration Incidents against the different priority levels and disapplying certain clauses which are not relevant for ECoS Migration Incidents.

1.6. Reporting

36. Section 4 of the ETMAD requires DCC to produce and maintain an ECoS Migration Reporting Regime (EMRR) that will, amongst other things, define the reports provided to Supplier Parties showing Failed Migrations and also those Device Models deemed to be Non-Migratable.

37. The EMRR will be developed as a stand-alone product defining the frequency and format of reporting to Supplier Parties.

38. Drafting within the ETMAD reflects the approach taken within the SMETS1 TMAD with the contents of the EMRR subject to industry consultation with an appeals route to the Secretary of State.

1.7. Provision of Information to the DCC

39. Section 5 of the ETMAD reflects the existing ETMAD drafting (that is currently in effect and incorporated into the SEC) requiring each Supplier Party to provide information the DCC reasonably requests and within such reasonable time period as the DCC may specify. At present no such requests have been made by the DCC.

1.8. Migration Approach

40. Section 6 of the ETMAD requires DCC to determine the approach to migration including, determining:

a) the mechanism for selecting Devices for ECoS Migration;
b) the mechanism 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, where activities referenced in (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 against 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 TCoS Certificate with an ECoS Certificate;
iv) reconciliation between ECoS Service Provider and TCoS Service Provider to confirm ECoS Migration has completed.

d) the controls in place to manage Failed Migrations, including the suspension of ECoS Migration for certain Device Models to allow issues to be investigated and prevent ECoS Migration for Devices deemed to be Non-Migratable; and
e) the mechanism for determining whether a Device Model should be categorised as Non-Migratable.

41. Each of these bullets are explained in further detail in the paragraphs below.

The mechanism for selecting Devices

42. The selection of Devices for ECoS Migration will be focused on each individual Device. Unlike SMETS1 migration, there is no requirement for Devices at a specific premise to be migrated together as the migration will be completed remotely with no consumer impact.

43. As set out in paragraph 19 of this consultation document, the ETMAD references specific exclusions where Devices will not be selected for migration. No further information on the selection approach has been included in the ETMAD. This reflects the simplicity of the arrangements, where the same approach will be applied for all Devices with no priority Devices or information required from Supplier Parties to support the selection process.

44. DCC has considered whether priority Devices should exist, for example whether Prepayment Devices should be identified and prioritised for proving activities ahead of Bulk Migration. In conclusion, it was agreed that the extra administrative effort associated with requiring Supplier Parties to identify Prepayment Devices was not justified given the minimal risk of Device functionality being impacted by the migration activities.

45. In line with this conclusion, DCC also considered whether Supplier Parties should be able to influence the choice of Devices and concluded that this would not be necessary as the transfer of certificates would take place in the background without impacting Device functionality.

The mechanism for initiating ECoS Migration in a controlled and managed way, ensuring successful migrations are achieved on a number of Devices before moving to Bulk Migration

46. Clause 6.1(b) in the ETMAD defines the minimum requirements for DCC proving activities before Bulk Migration of specific Device Model can commence.

47. DCC will follow a stepped migration approach where the DCC CoS Certificate will initially be transferred for a small number of Devices of a specific Device Model. This number will gradually increase as more Devices are successfully migrated. The actual number of Devices to be migrated to prove that Bulk Migration can commence will be dependent of the specific Device Model but will not exceed 300. This level of detail will be determined by DCC and not included in the ETMAD.

48. As the process followed for a TCoS to TCoS transfer is technically identical to a TCoS to ECoS transfer, it is proposed that successful TCoS to TCoS transfers will provide sufficient evidence to support Bulk Migration commencing for a Device Model.

49. The clause specifically defines the minimum expectations required by BEIS. These requirements allow DCC to commence Bulk Migration where proving activities have successfully demonstrated that a later version of firmware can be migrated. The assumption here is that, where DCC has demonstrated a later version of firmware can be migrated; it is acceptable to start Bulk Migration as any issues encountered can be resolved through a firmware upgrade.

50. The other minimum requirement specified within this clause is that, following the transfer of the DCC CoS Certificate, a CoS Update Security Credentials Service Request (SRV 6.23) has been successfully processed. The requirement to witness a successful change of supplier event will not be part of the standard migration process (i.e. a migration will be deemed to be successful once the ECoS and TCoS Parties have been reconciled). However, given the importance of the DCC CoS Certificate in the processing of an SRV 6.23, this requirement has been included as a restriction ahead of Bulk Migration, to mitigate the risk that high numbers of migrations take place leading to issues in the SRV 6.23 processing arrangements, that might have knock on impacts to consumers.

The steps required to successfully complete ECoS Migration

51. This clause identifies the high-level steps in the migration process. It is acknowledged that issues can occur at any of these steps leading to Failed Migrations. The approach taken to resolve these Failed Migrations will depend on the stage in the process where the failure occurred. This may require DCC or the Supplier Party to carry out remediation activities, as defined in the ECoS Migration Error Handling and Retry Strategy.

The controls in place to manage Failed Migrations

52. As part of its migration approach, DCC will ensure the technical solution allows timely suspension of ECoS Migration for certain Device Models where issues are identified. This will include 'all stop' functionality to prevent Devices of a particular Device Model being selected to enable issues to be investigated.

The mechanism for determining whether a Device Model should be categorised as Non-Migratable

53. A comprehensive approach to triaging migration issues will be defined, to support the DCC determination on whether issues encountered during migration can be resolved or whether the Device Model should be deemed to be Non-Migratable.

1.9. ECoS Migration Error Handling and Retry Strategy

54. Section 7 of the ETMAD requires DCC to produce and maintain an ECoS Migration Error Handling and Retry Strategy (EMEHRS) which will define the triage approach to be taken by DCC where there is a Failed Migration and the resolution activity that Supplier Parties should take.

55. Drafting within the ETMAD reflects the approach taken within the SMETS1 TMAD with the contents of the EMEHRS subject to industry consultation with an appeals route to the Secretary of State.

56. Detailed exclusions and error resolution actions will not be included within the ETMAD itself to allow flexibility as the migration commences and new types of error are identified where a standard resolution approach can be documented and applied consistently.

1.10. Comparison with SEC Section G11 Requirements

57. SEC Section G11.5 provides a high-level list of items that may be included in the ETMAD. In developing the ETMAD, DCC has considered this list, as shown in the table below:

Section G11 Requirement	Conclusion and Reference to Section of ETMAD

(a) rights and/or obligations of the DCC and other Parties designed to facilitate or achieve the purposes of the ECoS Transition and Migration Approach Document which are either additional to or vary other rights and/or obligations set out in this Code.	Section 1 includes rights and obligations associated with DCC carrying out ECoS Migration and resolving errors identified in relation to Failed Migrations. Section 1 also includes obligations on Supplier Parties to resolve issues identified.
(b) the processes by which SMETS2+ Devices that have been Commissioned will have their Device Security Credentials updated such that those security credentials which relate to the CoS Party will be derived from information contained in an ECoS Certificate instead of information contained in a TCoS Certificate.	Section 3 includes a change to SEC Section L allowing the TCoS Certificates to be replaced, linking to the existing process for replacing TCoS Certificates on expiry. As a single step migration, no additional technical details have been included.
(c) the processes by which changes to DCC Systems are to be made to enable the DCC to begin processing "CoS Update Security Credentials" Service Requests in relation to SMETS1 Devices.	Section 1 includes an obligation on DCC to provide information to the ECoS Party to enable them to process 6.23s relating to SMETS1 Devices.
(d) pre-conditions to apply in relation to the ECoS Migration of any SMETS1 or SMETS2+ Device, including by reference to the DCC, the Device Model, and/or the Responsible Supplier.	Clause 6.2(b) includes the approach to proving that migration has been successful before moving to Bulk Migration for a particular Device Model. No other pre-conditions have been identified.
(e) provisions enabling the DCC to process a 'CoS Update Security Credentials' Service Request in a different way, method or manner depending upon whether or not the Device in respect of which the Service Request is made has been ECoS Migrated.	Changes to Section 8 of the SRPD reflected in Section 3 of the ETMAD show the parallel approach to processing CoS Update Security Credential Service Requests for TCoS and ECoS Devices during the migration period.
(f) provisions that, from any such date as may be specified, permit or require any newly installed or Commissioned Device to have security credentials which relate to the CoS Party to be derived from the information contained in an ECoS Certificate instead of information that is contained in a TCoS Certificate.	Requirement included to prioritise installation of TCoS Devices held within a Supplier Party's inventory and cease install TCoS Devices 30 days prior to the end of the ECoS Migration Period. As referenced above, this is subject to ongoing discussions regarding the transfer of TCoS private keys to the ECoS Party. Depending on the outcome of these discussions, further changes to the ETMAD may be required.

(g) provisions requiring the DCC to report on its progress on ECoS Migration, including identifying whether in relation to Devices any particular category of Device Model and/or Device Type has failed, or is more likely to fail, ECoS Migration;	Section 4 includes a requirement on DCC to produce an ECoS Migration Reporting Regime setting out the frequency and format of reports to be provided during the ECoS Migration Period.
(h) provisions requiring the DCC to apply a specific strategy in respect of attempting to complete ECoS Migration for a Device in respect of which ECoS Migration has previously failed;	Section 6 includes a requirement on DCC to determine the approach to managing the migration including the selection of Devices, ramping up of migration activities and relevant controls to manage Migration Failures. The approach to dealing with Failed Migrations is also captured in the ECoS Migration Error Handling and Retry Strategy detailed in section 8.
(i) provisions requiring the DCC and Supplier Parties to take steps to resolve matters that are causing, or contributing to the cause of, failures of ECoS Migration;	Section 8 includes a requirement on DCC to produce an ECoS Migration Error Handling and Retry Strategy with Section 1 including an obligation on DCC and Supplier Parties to comply with this.
(j) provisions requiring the secure decommissioning of Systems of the TCoS Service Provider, for the revocation of any associated Organisation Certificates, and for the verifiable destruction of associated Private Keys;	The Go Live ETMAD does not include specific provisions regarding the de-commissioning of the TCoS Service Provider. This is subject to ongoing discussions between BEIS, DCC and its service providers.
(k) limitations and/or variations to the Services and/or the rights and/or obligations of the Parties to apply for a transitional period prior to and/or following the ECoS Migration of some or all Devices, which may include limitations and/or variations to Services in light of other proposed changes to this Code;	Section 3 includes transitional changes to specific SEC drafting to acknowledge the ECoS Migration and the parallel running of TCoS and ECoS processes.
(l) provision for the referral and determination of disputes in respect of the ECoS Transition and Migration Approach Document, which may include interim or final determinations by the Secretary of State, the Authority, the Panel or any other person specified by the Secretary of State.	Sections 1, 4 and 7 include the ability for Supplier Parties to appeal decisions to the Secretary of State regarding to Non-Migratable Devices, the content of the ECoS Migration Reporting Regime and the content of the ECoS Migration Error Handling and Retry Strategy, respectively.

1.11. Comparison with SMETS1 TMAD

58. The ETMAD has been developed in line with the general approach utilised within the SMETS1 TMAD. However, there are four key differences between the SMETS1 migration and the ECoS Migration which have resulted in a less complex migration approach. This section has been

included to explain those differences, to support industry review of the ETMAD drafting and address any potential questions on the differing provisions.

59. At a high level these differences include:

- Migration of a SMETS1 Installation includes multiple steps, delivered by different organisations, which could fail at any stage. Conversely ECoS migration is a single step process already captured within the SEC arrangements as a TCoS to TCoS replacement for expiring certificates. Therefore, the approach to managing migration failures will be less complicated.
- SMETS1 migration must be carried out on an entire SMETS1 Installation at once; whereas ECoS Migration will be done on a Device by Device basis.
- SMETS1 migration is dependent on activities being delivered by different actors including the Responsible Supplier, Installing Supplier, SMETS1 SMSO and DCC. In comparison, ECoS migration will be delivered by DCC and its service providers and will only be visible to Supplier Parties through post migration reporting.
- SMETS1 migration places the responsibility on Supplier Parties to authorise migration of Devices and provide information to DCC on priority installations. As the ECoS migration is enacted remotely with no impact on Device functionality, there is no need for Supplier Parties to authorise ECoS Migration. DCC and its service providers, will select the Devices to migrate and enact the certificate transfer with visibility provided to Supplier Parties through post event reporting.

60. A detailed comparison of the SMETS1 TMAD and ETMAD provisions has been included in Appendix 1.

3. Next Steps and Approval of the ETMAD

61. Following the closure of this consultation, DCC will consider respondents' views, and subject to the consultation responses received, submit to BEIS the ETMAD that it considers suitable for designation into the SEC, including why DCC considers the draft to be fit for purpose; copies of the consultation responses received; and any areas of disagreement that arose during the consultation process that have not been resolved.

62. Given the length of time between this consultation and the expected ECoS Service Live Date, we do not expect to submit the proposed ETMAD to BEIS immediately following the consultation. The EMRR and EMEHRS will be developed throughout 2022 and issued for industry consultation. This may result in additional changes required to the ETMAD. If this occurs, a further consultation will be issued ahead of submission to BEIS for designation.

63. As noted above, depending whether arrangements are made to transfer the TCoS Private Keys into the ECoS Party, a further version of the go-live version of ETMAD may need to be consulted upon.

4. Questions for Respondents

64. DCC would like stakeholders' views on the following consultation questions:

Q1	Do you agree with the DCC and Supplier Party rights and obligations set out in the proposed ETMAD? Please indicate any areas of disagreement and the reasons for them.
Q2	Do you agree with the timescales reflected in the definition of the ECoS Migration Period (June 2023 – November 2024) and the requirement on Supplier Parties to cease installation of TCoS Devices 30 days prior to the end of the ECoS Migration Period? Please indicate any areas of disagreement and the specific reasons for them e.g. volume of held stock.
Q3	Do you agree with the proposal that the DCC should stop delivering Communications Hubs with GPFs with TCoS Device Security Credentials by 225 days after the commencement of ECoS Migration?
Q4	Do you agree that the list of Non-Migratable Device Models should be published on the DCC Website publication on Non-Migratable. Please indicate any areas of disagreement and the reasons for them.
Q5	Do you agree with the approach to managing Non-Migratable Device Models, set out in the proposed ETMAD? Please indicate any areas of disagreement and the reasons for them.
Q6	Do you support the further assessment of the option to transfer the TCoS Certificate private keys to the ECoS Party? Please provide any specific points to feed into the business case.
Q7	Do you agree with the approach to developing the EMRR set out in Section 4 of the proposed ETMAD? Please indicate any areas of disagreement and the reasons for them.
Q8	Do you agree with the overall ECoS Migration approach set out in Section 6 of the proposed ETMAD? Please indicate any areas of disagreement and the reasons for them.
Q9	Do you agree with the approach to developing the EMEHRS set out in Section 7 of the proposed ETMAD? Please indicate any areas of disagreement and the reasons for them.
Q10	Do you have any further comments regarding the proposed ETMAD?

5. How to Respond

65. Please provide responses by 16:00 on 12 May 2022 to DCC at consultations@smartdcc.co.uk.

66. Consultation responses may be published on our website www.smartdcc.co.uk. Please state clearly in writing whether you want all or any part, of your consultation to be treated as confidential. It would be helpful to us if you could explain to us why you regard the information you have provided as confidential.

67. Please note that responses in their entirety (including any text marked as confidential) may be made available to the Department of Business, Energy and Industrial Strategy (BEIS) and the Gas and Electricity Markets Authority (the Authority).

68. Information provided to BEIS or the Authority, including personal information, may be subject to publication or disclosure in accordance with the access to information legislation (primarily the Freedom of Information Act 2000, the Data Protection Act 2018 and the Environmental Regulations 2004). If BEIS or the Authority receive a request for disclosure of the information we/they will take full account of your explanation (to the extent provided to them), but we/they cannot give an assurance that confidentiality can be maintained in all circumstances. An automatic confidentiality disclaimer generated by your IT system will not, of itself, be regarded by us as a confidentiality request.

69. If you have any questions about the consultation documents, please contact DCC via consultations@smartdcc.co.uk.

Appendix 1 – Comparison of SMETS1 TMAD and ETMAD Provisions

SMETS1 TMAD Section	ETMAD
Introduction and General Obligations	Section 1 covers the requirement for DCC to develop the ETMAD and the time over which the document will apply, reflective of the SMETS1 TMAD drafting. Section 1 also explains the scope of Devices covered by the ECoS Migration and the approach to excluding Devices. This approach differs within the SMETS1 TMAD and ETMAD to reflect the lower levels of complexity.
Definitions	New definitions applicable during ECoS Migration included in the ETMAD
Application of Section A (Definitions)	Amended definitions are included within the ETMAD. Where required, these reference clauses already amended via the SMETS1 TMAD (e.g. the definition of DCC Live Systems is amended by both the SMETS1 TMAD and the ETMAD). It is proposed that no change to the definition of Planned Maintenance or Responsible Supplier is required for the ETMAD.
Application of Section F (Smart Metering System Requirements)	This section of the SMETS1 TMAD reflects the approach to managing the SMETS1 Pending Product Combinations and SMETS1 Eligible Products Combinations lists. This is not relevant to the ETMAD.
Application of Section G (Security)	Whilst both the SMETS1 TMAD and the ETMAD impact Section G, the ETMAD changes are limited to re-introducing the exclusion for separation relating to the TCoS Party and the reference to TCoS Party alongside reference to the CoS Party to show the parallel running.
Application of Section H (DCC Service)	The SMETS1 TMAD amends Section H planned maintenance provisions, allowing DCC to undertake planned maintenance at any time provided a schedule is made available at least 10 working days in advance. Equivalent changes are not required for the ETMAD as ECoS Migration will not impact Supplier Parties management of Devices. Therefore, DCC can support the existing maintenance arrangements.
Application of Section L (Smart Metering Key Infrastructure and DCC Key Infrastructure)	Both the SMETS1 TMAD and the ETMAD introduce new Remote Party Roles to reflect the specific roles required to support SMETS1 and ECoS Migration. The ETMAD also includes an additional clause to introduce the ability for a DCC CoS Certificate change for the purposes of ECoS Migration.

Application of Section M (General)	The SMETS1 TMAD includes several paragraphs confirming the liabilities where the steps reflected in the TMAD result in loss of Data or impact the ability to utilise functionality of the Device. Whilst the ETMAD also includes reference to liabilities the specific clauses differ as follows: • Both the ETMAD and SMETS1 TMAD clarify that DCC and the Responsible Supplier shall not be liable when carrying out actions in accordance with Good Industry Practice. However, SMETS1 also references activities carried out by the Installing Supplier. This is not relevant for the ETMAD as the Installing Supplier is not involved in ECoS Migration. • The SMETS1 TMAD clarifies that the SMETS1 SMSO may permit DCC to take steps provided in the TMAD which result in communication of interference with the SMETS1 Installation. This clause is not relevant for the ETMAD as DCC will not make any changes to SMETS1 Devices. • The SMETS1 TMAD acknowledges that the SMETS1 SMSO is acting as a DCC Service Provider when performing tasks under the TMAD and can therefore rely on the waiver in Section M2.13(a) of the SEC. This clause is not relevant for the ETMAD as ECoS Migration does not require the SMETS1 SMSO to carry out specific actions; nor does it place requirements on any other organisation to act as a DCC Service Provider. • The SMETS1 TMAD requires both the DCC and the Installing Supplier to act in accordance with Good Industry Practice. An equivalent clause is included in the ETMAD relating to the DCC and the Responsible Supplier. • The SMETS1 TMAD requires the DCC to take reasonable steps to ensure that any data provided to it by the SMETS1 SMSO for the purposes of migration, is accurate. This clause is not relevant for the ETMAD as no data is provided by the SMETS1 SMSO. In addition, no other data is used for ECoS Migration by organisations other than DCC and its service providers. • The SMETS1 TMAD limits DCC and each Installing Supplier's liability for failing to act in accordance with Good Industry Practice, in relation to the migration of Dormant Meters, to £1m for each period of 12 months from the date the TMAD came into effect. There are no specific exclusions required within the ETMAD as the migration of specific Devices e.g. those associated with Dormant Meters, are not expected to require a different migration approach.
Application of Appendix AC (Inventory Enrolment and	Changes required to Appendix AC to recognise the TCoS Party and to switch off the new alert introduced with the ECoS arrangements which identifies Devices being installed with TCoS Certificates. These amendments do not impact the clauses being amended by the SMETS1 TMAD.

Decommissioning Procedures)	
Application of Appendix AG (Incident Management Policy)	The SMETS1 TMAD amends Appendix AG to recognise SMETS1 Migration Incidents. A similar approach has been taken within the ETMAD, to recognise ECoS Migration Incidents.
Pre Migration Rights and Obligations	The SMETS1 TMAD contains several requirements that support the overall migration process. These have been reviewed to determine whether similar requirements are needed for the ETMAD, as set out below: • The SMETS1 TMAD requires the Responsible Supplier to provide information regarding SMETS1 SMSOs migration activities to support DCC planning. In comparison, the ECoS Migration will be led by DCC and will not require the Responsible Supplier to authorise migration or provide any information regarding priority migrations. Therefore, only a single clause has been included within the Go Live ETMAD (reflective of the clause included in the existing ETMAD) which requires each Supplier Party to provide information reasonably requested by DCC. • The SMETS1 TMAD requires DCC to prioritise dormant meters over active meters. Such a prioritisation is not required for the ETMAD as SMETS1 Devices do not contain DCC CoS Certificates and are therefore not subject to ECoS Migration. • The SMETS1 TMAD refers to a list of Eligible Product Combinations specifying which Device Model Combinations are eligible for migration. Whilst the ETMAD doesn't include a list of Device Model Combinations that are eligible for migration, it does include similar provisions associated with Device Models that are categorised as Non-Migratable. As per the SMETS1 TMAD, a requirement has been included on the Responsible Supplier to upgrade the firmware to a version that can be migrated. In addition, the ETMAD requires DCC to confirm successful migrations on a later firmware version associated with a specific Device Model, before initiating Bulk Migration of Devices of that Device Model. • The SMETS1 TMAD includes a requirement on DCC to produce a Migration Authorisation Mechanism, for managing Responsible Supplier authorisations. As highlighted above, the ECoS Migration will be led by DCC and will not require the Responsible Supplier to authorise migrations. Therefore, a Migration Authorisation Mechanism is not required. • As the mechanism for authorising SMETS1 migration requires the Responsible Supplier to digitally sign its communications with DCC, there are provisions in the SMETS1 TMAD covering the use of IKI Certificates. Such provisions are not required in the ETMAD as the only communication envisaged between DCC and external parties will be the provision of reports,

	which will be provided via sharepoint and not require digital signing. • Both the SMETS1 TMAD and the ETMAD include a requirement on the DCC to produce a migration reporting regime, defining the format and frequency of reports to be provided by DCC to the Responsible Supplier. ETMAD drafting has been developed to be consistent with the approach taken within the SMETS1 TMAD. • The SMETS1 TMAD includes provisions relating to Electricity Distribution Network Operator Certificates IDs and change of Supplier events which are not applicable to the ECoS Migration.
Migration Process	The SMETS1 TMAD includes information regarding the migration approach, including activities to support the initial set up, digital signature of communications and the detailed process for migrating SMETS1 Devices. The equivalent clause within the ETMAD places the requirement on DCC to determine how devices are selected and how the migration is delivered. As highlighted above, this reflects the less complex migration with all activities delivered by DCC and its service providers. Within the ETMAD, there is no requirement for rolling back migration where errors arise as ECoS Migration is either a success or failure. Both the SMETS1 TMAD and the ETMAD include a requirement on the DCC to produce a migration error handling and retry strategy, defining the actions to be taken by DCC or the Responsible Supplier to resolve migration issues. ETMAD drafting has been developed to be consistent with the approach taken within the SMETS1 TMAD.
Commissioning Requirements and Commissioning Requests	The SMETS1 TMAD includes requirements on the Commissioning Party and DCC relating to the commissioning of SMETS1 Devices within the DSP. These are not applicable to the ECoS Migration on the basis that the ECoS Migration is a single step process with checks applied by DSP and confirmation that migration has completed using reconciliation between the TCoS Party and ECoS Party.
Decommissioning of a Requesting Party or the Commissioning Party	Discussions are ongoing regarding the de-commissioning of the TCoS Party. As such, the draft Go Live ETMAD is silent on these arrangements. A further version may be required to provide additional detail.
SMETS1 Migration Interface and Schema	The SMETS1 TMAD provides a schema detailing the definition of XML files which is not relevant to the ECoS Migration. However, ECoS Migration reporting will be provided via sharepoint, therefore reference to making data available to the relevant Responsible Supplier via sharepoint has been included within the reporting section of the ETMAD.
File Content Encryption and Decryption	The SMETS1 TMAD includes provisions relating to encryption which are not relevant to ECoS Migration.

Requirements Specific to certain Groups	The SMETS1 TMAD includes the concept of Group Ids to identify different types of Device (e.g. conditions in TMAD are varied for communication hubs). This concept is not required in the ETMAD as the same process will be applied across all Device Types with no need to vary obligations / rights.
SMETS1 Device Security Testing	The SMETS1 TMAD includes provisions relating to security testing which are not relevant to the ETMAD.
Excluded Categories	The SMETS1 TMAD details various exclusions where Devices are not eligible for migration. Equivalent clauses will not be included within the ETMAD; the detailed approach to resolving migration issues will be included in the ECoS Migration Error Handling and Retry Strategy to allow flexibility for DCC to define the approach as different migration issues are identified.