Data Communications Company

Response

to the DCC consultation on the draft "Go Live" version of the ECoS Transition and Migration Approach Document (ETMAD) – SEC Appendix AS

Date: 24 August 2022
Classification: DCC Public

Table of Contents

1. Introduction

1.1. Executive summary

1. On 11 April 2022, DCC issued a consultation seeking stakeholder views on 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. This document provides a DCC response to the industry comments received on the ETMAD consultation and sets out the current position and next steps regarding the further development of the Go Live ETMAD. We have discussed and agreed the contents of this consultation response document with the Department for Business, Energy & Industrial Strategy (BEIS), and will continue to engage with BEIS in relation to the ongoing activities.

3. Under the ECoS Programme, a significant amount of work is ongoing, including the development of further governance documents relating to the error handling approach and the reporting regime. DCC is also continuing to assess whether it is feasible for the TCoS Certificate private keys to be transferred to the ECoS Party. Therefore, based on the comments received on the Go Live ETMAD and following discussion with BEIS, we are not in a position to conclude on the drafting of the Go Live ETMAD at this stage. Once we have clarified plans and assessed the need or otherwise to adjust the Go Live ETMAD issued as part of this consultation, we will be conducting further engagement with industry. Our ambition is to have concluded this activity before the end of the year.

4. Where possible, DCC has included within this document the conclusions it has reached, in respect of the consultation questions asked regarding the Go Live ETMAD. Where work is ongoing, we have highlighted this within the response.

1.2. Background

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

6. When a gas or electricity consumer with a Smart Meter switches Supplier, the security information held on the Smart Meter needs to be changed so that it relates to the new Supplier 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 Transitional Change of Supplier (TCoS) processes and they are administered by part of the DCC Systems known as the "Change of Supplier Party" (CoS Party).

7. 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.

8. In 2021, DCC undertook a replanning exercise, resulting in changes to the ECoS Joint Industry Plan (JIP) milestones being issued for consultation with the Implementation Managers Forum in January 2022. 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.

Development of SEC provisions

9. 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].

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

11. Earlier this year, DCC 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 Procedures, 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]. Initial changes to introduce the DCC User Interface Specification v5.1 and Service Request Processing Document v7 were subsequently released on 30 June 2022, with further changes due at ECoS Go Live.

12. Within the conclusions document, DCC outlined that it has been developing the Go Live version of the ETMAD to be re-designated by BEIS 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 manage the initiation of dual running TCoS and ECoS Parties and the transition to ECoS and will:

- cease the suspension of the ECoS main body changes that have been introduced into the SEC;
- 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
- deal with other migration related matters such as the Device testing that needs to be carried out before a Device Model can be migrated in bulk and provisions for there to be a reporting regime and error handling strategy.

13. 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.

ECoS Programme Update

14. Following the appointment of the ECoS Application provider, DCC completed procurement activities in October 2021, with the Hosting and Service Management provider contract award. Work has progressed on the design, build and test phase of the ECoS Programme to deliver the enduring ECoS functionality, aligned to SEC provisions to be designated by BEIS for ECoS Go Live.

15. The development and delivery of the enduring ECoS solution is supported by a comprehensive testing phase, governed by the SEC Variation Testing Approach Document for the Enduring Change of Supplier Arrangements (ECoS SVTAD – SEC Appendix AR) and the associated Testing Approach Document.

16. BEIS has defined a set of Live Service Criteria which will be considered ahead of ECoS Go Live, with feed in from the relevant SEC governance bodies. This approach will ensure a robust solution is delivered, and the ECoS Party is ready to support the ECoS arrangements.

[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/

17. The ECoS Party will only be responsible for the processing of CoS Update Security Credential Service Requests (SRV 6.23s) in relation to Devices which hold ECoS Certificates. This will include newly commissioned Devices containing ECoS Certificates and previously commissioned Devices with TCoS Certificates that have been replaced with ECoS Certificates. The key purpose of the Go Live ETMAD is to govern the process for replacing TCoS Certificates, to ensure commissioned Devices are effectively 'migrated' from TCoS to ECoS; and to enable both the TCoS Party and the ECoS Party to process SRV6.23's during the migration period.

18. The actual mechanism for replacing the TCoS Certificate is based on existing functionality defined within the GBCS (TransCoSbyTransCoS command) for replacing the DCC CoS Certificate (or CoS Certificate)[1] to manage expiry of TCoS Certificates. Therefore, DCC is not expecting significant issues to arise as a result of the TCoS to ECoS Certificate replacement. A programme of work has already been delivered to replace TCoS Certificates[2] (housekeeping due to aging) and evidence from this activity is feeding into the ECoS Programme's analysis. DCC has also provided a GBCS Integration Testing for Industry (GFI) tool to enable Device Models to be tested against SEC functional requirements, including the ability to replace TCoS Certificates. We understand that a number of manufacturers / Suppliers have been using this tool and we would encourage Suppliers and manufacturers to make use of this tool to help provide additional comfort regarding the wholesale TCoS to ECoS Certificate replacement proposed by the ECoS Migration.

19. In preparation for ECoS Migration, DCC has initiated work to validate whether Device Models (a combination of manufacturer, model, hardware version and firmware version) are capable of accepting a TCoS to TCoS Certificate replacement command and can successfully process a subsequent Change of Supplier command. As at 31 July 2022, we have identified approximately 275 Device Models to be assessed (i.e. those that exist in production on that date), and have initiated TCoS to TCoS certificate replacements on the majority of these, with positive results and no Non Migratable Device Models found to date. We are also monitoring evidence of subsequent successful SR6.23 handling. Further detail on this analysis is currently being shared with industry.

20. This analysis supports DCC's expectation that the number of Non Migratable Device Models will be low (if any), with issues relating to specific Device Models being resolved via a firmware upgrade to a firmware version that is capable of accepting a DCC CoS Certificate replacement command. As reflected later in this document, DCC will be responsible for firmware updates relating to Communication Hubs and Supplier Parties responsible for upgrading other Devices.

21. However, we do acknowledge that attempts to migrate individual Devices may result in Failed Migrations due to wider issues with the specific Device e.g. communication failures. The ETMAD includes a requirement to provide a comprehensive suite of reports to enable Failed Migrations to be identified and remediation activities undertaken. Where the failure is due to the Device failing to accept the DCC CoS Certificate replacement command, we would expect a firmware upgrade to resolve the issue. Where the failure is due to an existing issue with the Device, not directly caused by the certificate replacement activity, then we would expect this to be resolved in accordance with existing mechanisms. Within DCC, a piece of work has been initiated to support the resolution of wider communication issues. This includes analysis regarding failed firmware upgrades to identify individual Devices where communication issues are preventing firmware upgrades from being applied. This result of this work is being shared with SEC Parties via the SEC Operations Sub Group.

[1] This is the generic term referenced in the SEC to cover either a TCoS or ECoS Certificate.

[2] Known as the TCoS to TCoS programme

2. Summary of Consultation Responses

22. Within its consultation document, DCC asked industry to consider ten questions, as set out below.

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 ECoS Migration Reporting Regime (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 ECoS Migration Error Handling and Retry Strategy (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?

23. In total, nine organisations (comprised of Meter Asset Providers (MAPs), Energy Suppliers and the SEC Panel) responded, providing direct responses to some, or all the questions.

24. Throughout the responses, a number of key concerns were highlighted relating to the overall ECoS Migration arrangements. These have been grouped into seven distinct themes, as summarised below.

Governance of the overall ECoS Migration approach

25. A number of respondents questioned the transparency of the ECoS Migration approach and requested clarity regarding the selection of Devices and the approach to ramping up ECoS Migration activities. In addition, the SEC Panel raised concerns regarding potential impacts on operational services and the need for clear delineation between the SEC Panel and BEIS governance activities.

DCC Response

26. The draft ETMAD requires DCC to determine the approach to delivering ECoS Migration, based on the expectation that there will be no operational impact on Devices as a direct result of the TCoS Certificate replacement. This expectation is based on the scope of activities required to 'migrate' a Device from TCoS to ECoS, which is essentially the replacement of the DCC CoS Certificate within the Device. The ability to replace the DCC CoS Certificate is existing functionality, not being introduced for the purposes of ECoS Migration, and has been successfully applied across a significant number of Devices. In addition, replacement of other security certificates is a business as usual activity carried out on a daily basis, for example with the replacement of supplier certificates and Access Control Broker (ACB) certificates. We would therefore not expect the replacement of certificates itself to impact the operation of the Device and will be carrying out appropriate testing of Device Models before their migration to validate this assumption.

27. Following the replacement of certificates, the Device will fall within the scope of the new ECoS Party, who will be responsible for processing SRV 6.23s submitted as part of a Change of Supplier event. The ECoS Programme is developing a comprehensive testing programme administered by the SEC Testing Advisory Group, covering the new ECoS Party function and this will be subject to formal sign off using the Live Service Criteria defined by BEIS. At the point ECoS goes live, the SEC Panel, DCC and BEIS will therefore have confidence in the ability of the ECoS Party to process SRV 6.23s without any operational impacts on Devices undergoing a Change of Supplier event following the installation of an ECoS Certificate.

28. DCC acknowledges concerns raised by respondents regarding the transparency of the migration approach and seeks to mitigate this concern by actively engaging with stakeholders to ensure a robust and transparent delivery of its regulatory requirements. We will make use of 'drop in' sessions with industry and presentations at governance groups, in particular the SEC Operations Sub Group and the Technical and Business Design Group (TBDG), to share information regarding the requirements built into the Device Candidate Selection Engine (DCSE) for the selection of Devices, and the overall delivery of ECoS Migration through the ramping up in the numbers of Devices to be migrated.

29. DCC has committed to providing progress reports to both BEIS and the relevant governance groups during the ECoS Migration Period. These reports will demonstrate the progress made against the overall migration plan and highlight any concerns that may impact delivery within the agreed milestone dates. At the SEC Operations Sub Group meeting on 12 July 2022, BEIS took an action to clarify its proposals for allocation of responsibilities during the migration process between itself and the various governance groups.

30. In response to the concerns regarding the criteria for progressing to Bulk Migration, the draft ETMAD reflects the minimum regulatory requirement i.e. where at least one Device of a particular Device Model has demonstrated a successful certificate replacement, there is comfort that the specific firmware version is capable of being migrated. This would demonstrate that there is no fundamental issue with a Device Model that is preventing a DCC CoS Certificate from being replaced. In practice, DCC is developing a stepped migration approach which ramps up the number of ECoS Migrations across Device Models before moving to Bulk Migration. Further information regarding this migration approach will be shared with industry through the wider stakeholder engagement sessions.

Migration Timeline

31. A number of respondents raised concerns regarding the timelines associated with ECoS migration, in particular they suggested completion of Bulk Migration within 10 months would be challenging. This position appeared to derive from concerns regarding the level of migration issues that may be encountered and also the level of TCoS stock that will continue to be installed following ECoS Go Live. Respondents highlighted the point that the enduring manufacturing pack will not be provided until ECoS Go Live, leading to a time lag where TCoS Devices will continue to be provided, particularly in the case of Communication Hubs.

DCC Response

32. DCC acknowledges concerns raised regarding the ECoS Migration timescales. We note that the approved JIP milestones include a 10 month timeline for completion of bulk migration, and we believe this timescale is achievable for the transfer of certificates for the commissioned TCoS Devices. However, recognising that there are likely to be individual Devices which are not easy to migrate and also that further TCoS Devices will be installed and commissioned following ECoS Go Live, we included within the draft ETMAD a further 5 - 6 months to manage resolution of 'difficult to migrate' Devices and to allow Suppliers to install remaining TCoS stock. DCC will monitor progression against the overall plan and flag any concerns to BEIS and the SEC Panel if required.

33. We have also been considering the approach for managing the de-commissioning of the TCoS Party, to avoid the need for a defined date within the ETMAD for ceasing the installation of TCoS Devices. Further information is provided in paragraph 48.

34. In relation to the point regarding the timescales for provision of the enduring manufacturing pack, this approach has been discussed and agreed with Supplier Parties to ensure testing is complete prior to Supplier Parties bulk ordering of ECoS Devices.

Stock Management

35. A key focus across the responses to several questions was the impact of ECoS Migration on stock management. Respondents requested clarity on how they would identify whether Devices contain TCoS or ECoS Certificates, both in relation to commissioned Devices and those provided by manufacturers following ECoS Go Live. Respondents also queried the timescales included in the draft ETMAD for the provision of Communication Hubs with ECoS Devices, requesting further detail on how this timeline had been derived.

DCC Response

36. In response to queries regarding the identification of ECoS versus TCoS Devices, DCC can confirm that, where a Device is Commissioned, a Supplier Party can verify the certificates recorded via the Smart Metering Inventory (SMI) for a particular Device using report RSMI_007. DCC will also be issuing reports to Supplier Parties, which will be specific to the ECoS Programme as defined in the ECoS Migration Reporting Regime (EMRR). These are intended to inform Supplier Parties on the progress of migration and will convey successful and failed migrations.

37. In preparation for a DCC pilot approach, we propose that Communications Hubs supplied for that purpose will be issued to parties supporting the pilot, with an additional indicator (likely to be a sticker on the body of the Communications Hub) to identify the Device as distinct from existing and subsequent shipments of TCoS stock.

38. We do not anticipate any further markings beyond the pilot nor any change to the Advance Shipment Notification. Once the ECoS Devices enter the supply chain, markers on those Devices would be of little advantage as, although they could be differentiated from older stock, there won't be any physical markings to differentiate migrated and unmigrated old stock. We therefore do not expect there to be reasonable justification for the cost of changing the physical attributes of Devices manufactured with ECoS Certificates.

39. Finally, we acknowledge concerns raised regarding the timescale reflected in the draft ETMAD, which gave a backstop date for the provision of Communications Hubs with ECoS Certificates as 225 days after the commencement of ECoS Migration. This timeline was determined based on the assumption that there will be a 6 week pilot which will allow a small number of installed ECoS Devices to be tested in production. Then DCC will request bulk delivery of ECoS Communications Hubs from the Communication Service Providers (CSPs). The CSPs have suggested that they require a maximum of 6 months to provide ECoS stock. In practice, we expect ECoS Devices to become available in advance of this date and we will commence the provision of these Communications Hubs as soon as possible to support Supplier Party stock management activities.

Categorisation of Non Migratable Device Models

40. In general, respondents stated that there was insufficient information available at this stage regarding the process for categorising Device Models as Non Migratable, with some noting that they would expect Supplier Parties to be involved in reviewing information regarding Device Models before they are added to the Non Migratable list.

DCC Response

41. DCC acknowledges the concerns raised by respondents regarding the processes for categorising Device Models as Non Migratable. As highlighted above, we have initiated analysis using data based on TCoS to TCoS Certificate replacements, to understand the level of Non Migratable Device Models. This analysis is indicating very low levels of expected issues, with no Device Models currently identified as Non Migratable.

42. However, it is possible that issues are identified during the ECoS Migration Period; therefore, we agree that it is important to have a robust and transparent process in place for determining whether a Device Model should be classified as Non Migratable.

43. We are currently developing the specific criteria and considering the level of industry involvement required within this process. Our expectation is that whether or not a particular Device Model is Non Migratable will essentially be a matter of fact that is established and demonstrated through testing or migration activities. The high level process for categorising a Device Model as Non Migratable will be set out in the externally facing ECoS Migration Error Handling and Retry Approach document[1] referred to within the draft ETMAD. Consultation on this document is planned for later in 2022.

Management of Failed Migrations for individual Devices

44. A key theme across the responses to multiple consultation questions was the approach to managing Failed Migrations in relation to individual Devices e.g. where the Device Model has been shown to have workable functionality to enable a TCoS to ECoS Certificate replacement, but the ECoS Migration still fails e.g. due to a communications issue. The main concern was that this would either lead to premature replacement of Devices or the Device would lose its smart functionality following the decommissioning of the TCoS Party.

DCC Response

45. DCC is keen to separate out Failed Migration of individual Devices from Device Models being categorised as Non Migratable. For the latter, as we have explained the population is expected to be very low, and we expect the decision to determine that a Device Model is Non Migratable to be clear cut, i.e. the specific Device Model is not capable of accepting a DCC CoS Certificate replacement command, or cannot subsequently process a CoS Service Request (6.23). Such an issue would be expected to impact all Devices with that particular Device Model. Where a successful certificate replacement has been seen on Devices for a particular Device Model but the

[1] This has been renamed from the ECoS Migration Error Handling and Retry Strategy to avoid confusion.

individual Device fails to migrate it is likely to be an issue for the particular Device itself and / or its communication links.

46. DCC is developing a retry strategy, where a number of migration attempts will be carried out where initial migration fails for a specific Device. This should help rule out any transitory issues impacting the success of the ECoS Migration. Details of the proposed retry strategy will be captured in the Migration Error Handling and Retry Approach document referred to within the draft ETMAD which will be issued for consultation at a later date.

47. Where migration for a specific Device continues to fail and the agreed number of retries have been completed, further analysis will be required to understand the root cause of the migration issues e.g. whether this is a known communication issue with the Device. The specific remediation activity to be carried out by either DCC or the Supplier Party will be dependent on the output from this analysis. As above, further details of the error handling approach will be captured in the Migration Error Handling and Retry Approach document referred to within the draft ETMAD which will be issued for consultation at a later date.

48. We also acknowledge the concerns regarding the potential premature replacement of Devices where they are not capable of receiving the ECoS Migration. As mentioned within the consultation document, we are considering an option to mitigate the risk that Devices will be stranded with TCoS Certificates at the point the TCoS Party is de-commissioned. This option might require the transfer of the TCoS Certificate 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 additional security risks that this may introduce. As this analysis is still ongoing, we have agreed with BEIS that it is not yet possible to conclude on the Go Live ETMAD at this stage. Further communications will be issued once we have sufficient clarity on the feasibility of this option and have developed any changes to the draft Go live ETMAD subsequently required.

Responsibility / liability for remediation activities

49. A number of respondents requested clarity on the approach to managing migration issues, noting that the error handling strategy was not yet available. In particular questions were asked regarding the responsibility for resolving issues relating to Communication Hubs; both in terms of resolution of issues encountered with the migration of Gas Proxy Functions with TCoS Certificates and also the responsibility for resolving migration issues relating to other Devices caused by issues with the relevant Communications Hub.

DCC Response

50. The draft ETMAD differentiates between Non Migratable Device Models and issues with individual Devices. Should any Device Model be categorised as Non Migratable, responsibilities would be as follows:

- DCC is responsible for firmware issues associated with Communications Hubs preventing TCoS Certificate transfer. In this scenario a remote firmware upgrade will be applied.
- Supplier Parties are responsible for firmware issues associated with other Devices preventing TCoS Certificate transfer. In this scenario, we would expect the Supplier Party to arrange for a firmware upgrade to be applied.

51. There will be instances where migration of individual Devices is not possible e.g. where the Device Model has been shown to have workable functionality to enable a TCoS to ECoS Certificate replacement, but the ECoS Migration still fails e.g. due to a communications issue. There may also be scenarios where a firmware upgrade cannot be applied due to existing communications issues.

52. Although not an ECoS migration issue, communication issues impacting individual Devices will prevent TCoS Certificates from being replaced, which may lead to Devices retaining TCoS Certificates and with no other intervention, losing smart capabilities following a change of supplier. DCC is investigating existing issues impacting Device communications and plan to present the output from this work to the SEC Operations Sub Group in the next few months. This issue also feeds into the ongoing considerations regarding the potential transfer of the TCoS Certificate private keys to the ECoS Party.

Reporting

53. Respondents acknowledged that full details of the reporting regime have not yet been published. However, based on the high level information contained in the draft ETMAD, one respondent requested that reporting should also cover the number of Devices yet to be migrated, not just details of those that have been migrated. The MAP respondents also requested that further consideration be given to the provision of reports to MAPs to enable them to understand the migration status of their assets.

DCC Response

54. Although the EMRR has not yet been formally shared for industry consultation, details of the proposed reports have been shared with industry through 'drop in' sessions and the ECoS summit. The expectation is that this product will cover the automated reporting to Supplier Parties regarding the status of Devices for which they are responsible.

55. In response to the request for reporting to Supplier Parties to also cover the number of Devices yet to be migrated, DCC is considering potential changes to the reporting for inclusion in the EMRR to provide further visibility to Supplier Parties regarding the type of certificate applied to their Devices. This will be particularly useful for Supplier Parties who gain Devices through a CoS event and also for newly Commissioned Devices where the Supplier Party is not clear whether an ECoS or TCoS Device has been installed.

56. In addition to the Supplier Party reporting, DCC will also provide regular migration updates to BEIS and the relevant governance group(s) e.g. the SEC Operations Sub Group and TBDG.

57. In relation to MAP reporting, DCC notes the reference to Modification Proposal 181 'Meter Asset Provider access to asset related data held by the DCC' and has considered this, in discussion with SECAS and MAPs. We understand the desire for MAPs to have access to information directly in relation to the status of their Devices and the work that has been completed to date by the MP181 working group to design a solution enabling this. We have therefore concluded that the most robust mechanism for providing data relating to the ECoS Migration status of individual Devices to MAPs, would be to use the mechanism being developed for MP181. The MP181 solution requires MAPs to request the new report for specific Devices based on the MAP providing a list of GUIDs. It is proposed that, for the period of ECoS Migration, the data provided within the MP181 report will be enhanced to include details of whether the Device contains a TCoS or ECoS Certificate, and where a Failed Migration has occurred, the report will also contain the latest error code. This enhanced reporting will be reflected within the ETMAD as a change to Clause H17.5[1] of the SEC whilst the ETMAD remains in force.

Conclusions

58. In this summary of consultation responses, DCC has provided a response in relation to the 7 key themes identified in responses to the Go live ETMAD consultation. Whilst we are not currently able to conclude on the full Go Live ETMAD drafting, we have, in discussion with BEIS, concluded the following:

[1] This is a new clause added as a result of Modification Proposal 181.

- The governance regarding the ECoS Migration Reporting Regime and ECoS Migration Error Handling and Retry Approach as set out in the draft ETMAD will apply, noting that the content of these documents is yet to be agreed.

- The Go Live ETMAD will differentiate between Non Migratable Device Models and Failed Migrations in relation to individual Devices; with DCC establishing the approach to classifying Device Models as Non Migratable and the resolution approach for dealing with Failed Migrations, within the ECoS Migration Error Handling and Retry Approach. It should be noted that the underlying process for classification of Device Models as Non Migratable set out in ETMAD is that DCC would identify any Device Models as such (in accordance with the approach DCC is to set out) and provide a justification for any such classification. If any Party disagrees with the classification, then DCC would seek to reach agreement with that Party over the classification and in the event that this was not possible, the matter could be referred to the Secretary of State for a determination.

- No changes are proposed to section 3 which covers the transitional changes to existing SEC provisions for the ECoS Migration Period.

- No changes are proposed to section 6 which defines the minimum regulatory requirements placed on DCC to manage the ECoS Migration, noting that further detail will be shared through stakeholder engagement activities including regular updates to the SEC Operations Sub Group and / or TBDG.

- Further work is required to determine the approach to managing the de-commissioning of the TCoS Party. We anticipate that the agreed solution may result in changes to section 1 of the ETMAD, in particular the obligations on Supplier Parties to cease installation of TCoS Devices (including considering whether any such obligation will be necessary at all in light of the further work on options for re-use of the TCoS private keys by the ECoS Party). We therefore believe a further consultation on impacted ETMAD clauses will be required later in the year.

3. Next Steps

59. In parallel with the publication of this document, DCC has provided a summary of responses to BEIS. As outlined in the executive summary, DCC has also discussed the current position regarding the development of the Go Live ETMAD with BEIS.

60. Given the ongoing work to deliver the ECoS Migration Reporting Regime and the ECoS Migration Error Handling and Retry Approach, in addition to the consideration of the possible transfer of TCoS Certificate private keys to the ECoS Party; it has been agreed that it is too early to conclude finally on the content of the Go Live ETMAD. We therefore expect to issue a further consultation regarding the required provisions relating to the de-commissioning of the TCoS Party either to enable this information to be included in the Go Live ETMAD or for a subsequent version.

61. DCC will continue to engage with industry through 'drop in' sessions and SEC governance groups as these activities progress with a further industry consultation planned later this year.