Data Communications Company

Consultation

SEC Subsidiary Document Changes required for the Enduring Change of Supplier (ECoS) Arrangements

Date: 24.09.21
Classification: DCC Public

Table of Contents

1. Purpose of this consultation

This consultation seeks stakeholder views on changes to the following Smart Energy Code (SEC) Subsidiary Documents required for the "Enduring Change of Supplier" (ECoS) arrangements:

- DCC User Interface Services Schedule (Appendix E)
- Threshold Anomaly Detection Procedures (Appendix AA)
- Service Request Processing Document (Appendix AB)
- Inventory Enrolment and Decommissioning Procedures (Appendix AC)
- DCC User Interface Specification (Appendix AD).

This consultation overview document summarises and seeks stakeholder feedback on the proposed changes. The proposed changes to the SEC Subsidiary Documents listed above are attached to this consultation. The changes will be 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 "Transitional Change of Supplier" (TCoS) to ECoS can commence, and after considering any feedback.

This consultation also seeks views on a change to the initial version of the ECoS Transition and Migration Approach Document (ETMAD) that BEIS has previously consulted on. The initial version of the ETMAD is planned for designation at the time when the current SEC main body changes for ECoS that are currently before Parliament are due to come into effect in mid-October 2021.

Lastly, this consultation seeks an indication from Supplier Parties, whether they intend to carry out testing of User Systems to verify that they can successfully submit 'Update Security Credentials (CoS)' Service Requests under the ECoS arrangements and have them successfully processed.

The closing date for this consultation is Friday, 5 November 2021. We do however require any views in response to Question 2 of this consultation (regarding the ETMAD) by 13 October 2021.

2. Background and context

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

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

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. Following this consultation, the Secretary of State approved the *Delivery Plan for Enduring Change of Supplier*[1] on 30 March 2020.

[1] https://www.smartdcc.co.uk/customer-engagement/consultation-on-the-delivery-plan-for-enduring-change-of-supplier-1/

2.1. Approach to the Implementation of the SEC Changes for ECoS

The introduction of the ECoS arrangements require 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. For brevity, those changes are not repeated here. The BEIS response to its consultation was published on 15 June 2021 and can be found in the following link:

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/

The changes to the SEC are being made using powers under Section 88 of the 2008 Energy Act. As outlined in the BEIS consultation, SEC Subsidiary Document changes required will also be made using powers under Condition 22 of the DCC Licence and Section X5 of the SEC.

Aside from future versions of the ETMAD that will need to be redesignated, DCC and BEIS have reviewed SEC Subsidiary Document changes required for the ECoS Arrangements and consider the changes outlined in this document to be the entirety of what is required at present.

For completeness, Section 2.2, Section 2.3 and Section 2.4 of this consultation document outline other SEC Subsidiary Documents necessary to support the ECoS arrangements that: have already been designated; have been consulted on and will soon come into effect; and that will need to be redesignated in the future.

2.2. The ECoS SEC Variation Testing Approach Document (SVTAD) has been designated

DCC issued a consultation between 14 April 2021 and 14 May 2021 seeking views on the draft SVTAD for the ECoS arrangements. Following consideration of consultation responses received, DCC published a consultation conclusion document and submitted the ECoS SVTAD to the Secretary of State on 4 June 2021. The ECoS SVTAD came into effect on 30 July 2021.

The ECoS SVTAD is a high-level framework for testing arrangements and requires the production of a Testing Approach Document (TAD), to contain the detailed testing approach developed by the DCC. DCC is currently drafting the TAD and the SEC Panel's Testing Advisory Group is being kept informed accordingly.

In the DCC *Delivery Plan for Enduring Change of Supplier*, we outlined that DCC would produce a User Test Services Approach Document (UTSAD) for ECoS and consult with SEC Parties. However, as outlined in the DCC ECoS SVTAD consultation conclusion document, it is DCC's expectation that Supplier Parties will wish to do this themselves, without the need to be mandated to do so. DCC considers that User Testing will need to focus on Users' ability to successfully run Change of Supplier Update Security Credentials Service Requests (SRV 6.23) under the new ECoS arrangements.

If, in the unlikely situation that DCC considers that Mandated User Testing is required, prior to the implementation of the ECoS changes going live, DCC will set out its proposals for User Testing in a draft ECoS Mandated User Testing Document. This would include those Users that should be required to participate in the testing and the User Role in which they are required to participate. It would also include the approach to testing; the arrangements for test completion; the process for

resolving test disputes; and notification of test completion. In that event, DCC would also ensure that sufficient notice would be given to allow appropriate time for preparation.

DCC, through this consultation, is seeking confirmation, or otherwise, from Supplier Parties on their intention to carry out testing of User Systems, to verify that they can successfully submit "CoS Update Security Credentials" Service Requests under the ECoS Arrangements and have them successfully processed.

DCC would greatly appreciate an early indication from Supplier Parties (in response to this consultation) of their intention to participate in ECoS testing. Responses from Supplier Parties on whether they intend to carry out testing of User Systems will help DCC make an informed decision as to whether a draft Mandated User Testing Document may need to be consulted on.

As was outlined in DCC's conclusions on the ECoS SVTAD consultation, any ECoS Mandated User Testing Document implemented would first require consultation with the Testing Advisory Group, Parties, and other relevant stakeholders, before submission of plans to the Secretary of State. If this unlikely situation should occur, we would make best endeavours to ensure that a range of Supplier Parties would participate in a robust, fair, and equitable manner.

DCC also considers that any obligation placed on Users should allow a reasonable time for those Users to prepare for mandated testing (should it need to be introduced) with their own systems and potential Service Providers.

For clarity, DCC also considers that no amendment is needed to the Common Test Scenarios Document (CTSD). In the *Delivery Plan for Enduring Change of Supplier* we outlined that DCC would update and consult on any changes required to the CTSD. On further review, DCC considers that the CTSD does not need to be amended as Service Reference Variant (SRV) 6.23 Update Security Credentials is within the test scope for new entrants, in Supplier roles, undertaking User Entry Process Testing (UEPT). The changes to SRV 6.23 Update Security Credentials to support the ECoS Programme are not deemed to be sufficient to warrant existing DCC Users in Supplier roles being asked to retest under the CTSD framework.

DCC encourages parties to test the changes in the ECoS User Testing window where possible. We have reviewed the Enduring Test Approach Document (SEC Appendix J) and no updates are needed to support the ECoS arrangements.

Question 1	**If you are a Supplier Party, do you intend to carry out testing of User Systems in order to verify that you are able to successfully submit 'Update Security Credentials (CoS)' Service Requests under the ECoS arrangements and have them successfully processed?**

2.3. We are seeking views on an amendment to the first version of the ECoS Transition and Migration Approach Document (ETMAD) that has previously been consulted on by BEIS and is due to take effect in mid-October 2021

In its 1 April 2021 consultation, BEIS consulted on a new SEC Subsidiary Document – the ECoS Transition and Migration Approach Document (ETMAD). The ETMAD is planned to be used to control the process of transition and migration to ECoS. However, it should be noted that the primary purpose of the first version of the ETMAD is essentially to undo the ECoS related main body SEC changes that were also consulted on, during BEIS' April 2021 consultation.

BEIS proposed a designation date for the first version of the ETMAD and the ECoS related SEC main body changes (as they are intended to coincide) as being 28 September 2021, or as soon as practicable within two months thereafter. DCC has discussed the designation date with BEIS and the changes are currently before Parliament. Subject to Parliamentary processes these changes are due to take effect from mid-October this year (rather than at the end of September). The relevant document changes can be found in the following link:

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/.

The ECoS related SEC main body changes to Section G require the DCC to develop an ECoS Interface Specification and to publish it on the DCC website.

The ECoS Interface is an important security interface and, whilst accepting that there is a need to produce and maintain the interface specifications, in discussions with BEIS, DCC has raised questions regarding whether it is appropriate to publish the details of the interface in the public domain. Subject to reviewing the responses to this consultation, BEIS has provisionally agreed with DCC that instead of requiring the interface specification to be published on the DCC website, a more appropriate arrangement would be to require the document and any supporting Security Impact Assessments to be made available to the DCC independent Security Assessment Service Provider for review, as part of carrying out a DCC Security Assessment.

It should be noted that ECoS only has interfaces with Users. Consequently, the ECoS Interface Specification is not a specification that any Users need to build their systems. A security impact assessment of the implications of the initial ECoS Interface and any subsequent changes to it are also reviewed by the Security Sub-Committee.

Views are therefore invited on using the ETMAD to make a change to the SEC Section G obligations relating to the publication of the ECoS Interface Specification.

Question 2	**Do you have any views on amending the first version of the ETMAD to make a change to the SEC Section G obligations relating to the publication of the ECoS Interface Specification (i.e. that rather than DCC publishing the ECoS Interface Specification on the DCC website, requiring that it and any supporting Security Impact Assessments be made available to the DCC Independent Security Assessment Service Provider for review, as part of carrying out a DCC Security Assessment)?** ***Please note that we require any views in response to this question by 13 October 2021 so that those views can be considered by DCC and BEIS prior to the first version of the ETMAD taking effect in mid-October 2021.**

2.4. A future "Go Live" version of the ETMAD will be consulted on in Q1 2022

As discussed above, the initial version of ETMAD is planned for designation in mid-October 2021 to coincide with the main body SEC changes for ECoS. A further "Go Live" version of the ETMAD will be consulted on and brought into effect for the commencement of ECoS Migration currently planned for June 2022. This version of the ETMAD would:

- cease the suspension of the ECoS main body SEC changes that BEIS has consulted on;
- set out the arrangements whereby SRV 6.23s are processed differently by DCC depending on whether the target device holds Device Security Credentials are ECoS related or TCoS related; and
- deal with other migration related matters.

BEIS had previously proposed a consultation for the "Go Live" version of the ETMAD in Q4 2021, however we consider it prudent to avoid consulting over the Christmas and New Year period and are now proposing that this consultation should take place in Q1 2022.

DCC will carry out briefings in December 2021 and January 2022, to ensure that Parties can contribute to discussion on ECoS migration related matters that are to be covered in a "Go Live" ETMAD, prior to any formal consultation undertaken by DCC or BEIS. DCC therefore expect to consult on the "Go Live" version of the ETMAD in Q1 2022 and are targeting a consultation commencement date of 4 February 2022.

DCC would also encourage Parties to join the twice monthly drop-in sessions on 'Migration & Devices' and 'Design, Build and Test' to continue discussions with DCC on areas of interest to you related to the ECoS Programme.

3. Summary of the proposed ECoS-related SEC Subsidiary Document Changes that we are seeking feedback on in this consultation

The ECoS related SEC Subsidiary Document amendments that are being proposed in this consultation are to:

- DCC User Interface Services Schedule (Appendix E)
- Threshold Anomaly Detection Procedures (Appendix AA)
- Service Request Processing Document (Appendix AB)
- Inventory Enrolment and Decommissioning Procedures (Appendix AC)
- DCC User Interface Specification (Appendix AD).

A summary of each of the proposed changes is described below. The proposed wording amendments to the documents are appended to this consultation summary document.

3.1. DCC User Interface Services Schedule (Appendix E)

A change is proposed to the DCC User Interface Services Schedule (UISS) to increase the Target Response Time for 'Update Security Credentials (CoS)' Service Requests (Service Reference Variant (SRV) from 30 seconds up to 35 seconds where the target Device is a SMETS2+ Device, and from 16 seconds to 21 seconds where the Target Device is a SMETS1 Device.

The proposed increase in Target Response Times reflects the additional processing and message routing needed for SRV 6.23s following the introduction of ECoS. It also includes additional time to allow the new CoS Party to perform the updated required processing steps. The existing Target Response Times do not include the additional time that will be required for the new ECoS Party and the associated network timing both ways between the ECoS Party and Data Service Provider (DSP).

DCC is proposing an amendment to the Target Response Times, as outlined in the UISS, as the most economic and efficient means of resolving this issue because DCC considers that this option will have little or no impact on Users. An alternative option that DCC has investigated is to decrease the processing time within the DSP (which is part of the overall Target Response Time). However, this option is not considered to provide value for DCC customers as it will require a contractual change with the DSP and significant cost increase.

Question 3	**Do you have a view on whether the increased Target Response Times for 'Update Security Credentials (CoS)' Service Requests (Service Reference Variant (SRV) 6.23) will impact User operations? If you do consider there is an impact, please explain your rationale.**

Question 4	**Do you agree with the proposal to increase the Target Response Times 'Update Security Credentials (CoS)' Service Requests (Service Reference Variant (SRV) 6.23) from:** • **30 seconds to 35 seconds where the Target Device is a SMETS2+ Device?; and** • **16 seconds to 21 seconds where the Target Device is a SMETS1 Device?** **If you do not agree with this proposal, please indicate why.**

3.2. Threshold Anomaly Detection Procedures (Appendix AA)

A number of changes to the Threshold Anomaly Detection Procedures (TADP) are proposed, not all of which are directly related to the introduction of the ECoS Arrangements, but which instead are intended to clarify the default position. The following changes are proposed as file checks:

- First that an anti-replay check is applied by the DCC, by requiring the DCC to check that the sequence number in any anomaly detection file from a User (acting with a particular User ID) is greater than that in any previous file that has been successfully processed by the DCC in relation to that User ID.

- Second, that the DCC will check that an Anomaly Detection Threshold (ADT) file does not contain more than one entry for a particular SRV with the same Time Period as another entry.

In the event that the file passes these checks then further processing will be carried out as a part of the file load:

- Whilst loading any new file with a higher sequence number than an existing file, where an ADT file does not include an entry relating to a SRV that gives rise to a critical command, the DCC should create one with an ADT and Warning Thresholds of zero and Time Period Applicable of 1440 minutes (1day).

- For SRV 6.23 (CoS Update Security Credentials), if there is no entry corresponding to a Time Period Applicable of 1440 minutes (1 day), the DCC should create an entry for that Time Period Applicable with an ADT and Warning Threshold of zero.

- If no ADT file has even been submitted by a User acting using a particular User ID, the DCC should set the ADT and Warning Threshold values to zero (with a Time Period Applicable of 1 day) for all SRVs that give rise to critical commands.

- It is also clarified that for other SRVs (i.e. those not giving rise to a critical command) if there is no entry in a particular ADT file, the DCC will not set an ADT or Warning Threshold value for that SRV.

Clause 3.7 has also been modified to make it clear that if any of the checks fail, the DCC would reject the ADT file in its entirety.

A change has been made to the content of the CSV file to require a Sequence Number to be included, for use by the DCC in applying anti-replay checks. For any particular User ID, this would need to be set to be greater than any previously successfully processed ADT file for it to be successfully processed.

The result of these changes is that as a minimum there will always be an ADT value for each SRV that gives rise to a critical command. For other SRVs, there will be no ADT or Warning Threshold value if no entry is included for that SRV in the latest ADT submission from a User acting with a particular User ID and the DCC would not "default" to retaining any previously set values for those SRVs.

It is noted that, despite the requirements of SEC Section G6.3(a)(ii), it is not proposed that where a User fails to submit an ADT value in relation to a SRV that results in a non-critical command but which does give rise to a Service Response that contains encrypted data, the DCC would not set out a default ADT and Warning Threshold value of zero.

Users may wish to test their ability to set appropriate ADTs under the new arrangements prior to their switch on at ECoS live.

Question 5	**Overall, do you support the proposed amendment to the TADP as outlined in this consultation? If you do not, please indicate any areas of disagreement and reasons for them.**

3.3. Service Request Processing Document (Appendix AB)

Changes are proposed to the Service Request Processing Document (SRPD) for ECoS. The redlined version of the SRPD attached to the consultation includes changes that are being made in support of the new ECoS solution as well as additional linked changes that are included under SEC Modification Proposal 104 (MP104), specifically changes associated with SRV 6.23 (CoS Update Security Credentials) are included – i.e. to. confirm that the Certificate used to Check Cryptographic Protection for the Service Request has a Remote Party Role of "xmlSign";

In addition, the following checks have been added for SRV 6.23s:

i) A check that the User ID in the Service Request is the same as that in the Certificate that was used to successfully check the Digital Signature on the Service Request;

ii) A check to confirm that the Market Participant Identifier (MPID) used to carry out the Registration Data look-up (to confirm that the supplier sending the Service Request is an incoming supplier for the relevant device) is the same as an MPID in the Certificate that was used to successfully check the Digital Signature on the Service Request. This means that suppliers with multiple MPIDs will need to use the correct Private Key to sign the Service Request (i.e. the one whose corresponding Certificate contains the MPID that is associated with the relevant device in the registration data);

iii) A check to confirm that the MPxN in the Service Request is the same as the MPxN associated with the target device in the Smart Metering Inventory;

iv) A check that the requisite number of replacement Certificates are included within the Service Request for the target device type;

v) A check to confirm that all of the replacement Certs have a Remote Party Role corresponding with that of a "supplier";

vi) Confirmation that the key usage of the replacement certificates is appropriate for the Trust Anchor Cell that they are being used to populate; and

vii) Where a prepayment key is being replaced, that the "SupplierPrepaymentTopUpFloorSeqNumber" data item is included.

A number of generic changes are proposed for all Service Requests that include Certificates which are to be used update the Device Security Credentials of a Device (this includes but is not limited to SRV 6.23s). These are to include the following additional checks:

i) That for each Organisation Certificate included within the Service Request, the Issuing Organisation Certificate Authority (OCA) Certificate is also included (so that the Device can Confirm Validity for the Certificate);

ii) That each Issuing OCA Certificate included within the Service Request has been used to Issue at least one of the Organisation Certificates in the Service Request.

Clause 8.1 sets out the checks to be applied by the CoS Party to a Countersigned CoS Service Request it receives from the DSP. Many of these replicate the checks applied by the DSP itself to the original Service Request. It should be noted that, in contrast to existing arrangements, under ECoS, these checks are applied to Service Requests targeted at SMETS1 Devices as well as SMETS2+.

If the checks are successful, Clause 8.2 requires the CoS Party to apply CoS Party Anomaly Detection as set out under Clause 20. The CoS Party only applies User-set ADTs, not global thresholds, and furthermore only applies thresholds set for a Time Period Applicable of 1440 minutes (1 day). If CoS Party Anomaly Detection fails (i.e. the threshold is exceeded) the CoS Party ceases processing of the Service Request (and an alert is sent to the relevant user) and no quarantining applies – and hence the relevant supplier will need to re-send the Service Request if it still wishes to change the credentials on or in relation to the relevant device.

Where the CoS Party checks succeed, the CoS Party generates a CoS Authorisation Response and returns this to the DSP. In the case of SMETS1, this is essentially just the original Service Request countersigned by the CoS Party. In the case of SMETS2+, this additionally includes an Update Security Credentials Pre-Command signed by the CoS Party.

Clause 8.4 sets out the checks that the DSP applies to a CoS Authorisation Response and, subject to the checks being passed, requires the DSP to apply anomaly detection and (again subject to this being passed) either (for SMETS1) send a Countersigned Service Request to the relevant SMETS1 Service Provider or (for SMETS2+) send a Command to the relevant Device.

Question 6	**Overall, do you support the proposed amendment to the SRDP as outlined in this consultation? If you do not, please indicate any areas of disagreement and reasons for them.**

3.4. Inventory Enrolment and Decommissioning Procedures (Appendix AC)

The proposed change to the Inventory Enrolment and Decommissioning Procedures (IEDP) are to:

- change the description of the Organisation Certificate with a remote party role of "transitionalCoS" to be a DCC CoS Certificate (rather than DCC Transitional CoS Certificate). Note the actual remote party role description remains as "transitionalCoS", since we wish to avoid having to change the GB Companion Specification for these purposes; and

- require DCC to send an alert to the relevant supplier where the DCC identifies that a Trust Anchor Cell of a Device, that has been added to Device Log of a Communications Hub Function, has been populated with Security Credentials derived from a DCC CoS Certificate that has a subject field that is populated with an identifier of a DCC Service Provider that does not provide services to the CoS Party, to notify them of the situation, so that subsequent action can be taken before the installing party completes the install and commissioning proves and leaves site.

Question 7	**Overall, do you support the proposed amendment to the IEDP as outlined in this consultation? If you do not, please indicate any areas of disagreement and reasons for them.**

3.5. DCC User Interface Specification (Appendix AD)

Changes are proposed to the DCC User Interface Specification (DUIS) to create an updated DUIS version 5.1 to include changes arising from both ECoS Solution support and wider changes relating to Modification Proposals targeted for inclusion as part of the June 2022 SEC Release (including updates associated with MP0104, SECMP0024 and SECMP00015). The redlined version of the DCC User Interface Specification (DUIS) reflects the proposed complete set of currently known changes for this updated DUIS v5.1 in order to reflect the entire scope of the interface changes and not just those associated with the ECoS changes to aid User readability and avoid any confusion.

The changes include:

- Additional Defined Terms have been added into section 1.3 for *ECoS Party* and *XML User Role Signing Private Key*

- Updates have been made to Section 2.53 for Message Authentication and section 3.3.1 for DUIS XML Service Request Signing, to introduce an additional Response Code (E65) to validate the Remote Party Role of the User Certificate used to sign all Service Requests to the DCC, to check that the Remote Party Role of the User's Organisation Certificate is 'xmlSign'.

- Seven (7) additional Response Codes has been added to section 3.5.10 for Service Response codes generated by DCC to include new Response Codes E65, E66, E67 E68, E69, E70 and E71
- DCC Alert Codes Section 3.6.3.4 has been updated to include:
    - DCC Alert Code N26 has had its trigger conditions extended to cover additional ECoS scenarios
    - New DCC Alert Codes N63 and N65 and associated definitions have been added to support the proposed ECoS solution
    - New DCC Alert Code N64 and associated definitions have been added to support SEC Modification SECMP0024.
- The new additional DCC Alert Codes and Response Codes have been added to section 3.6.4 to update the Relationship between DCC Alert Codes and Response Codes
- The Service Request Definition for SRV 4.18 *ReadMeterBalance* in section 3.8.42 has been updated to reflect changes associated with SEC Modification SECMP0015.
- The Service Request Definition for SRV 6.23 *UpdateSecurityCredentials(CoS)* in section 3.8.76 has been updated to reflect changes associated with the proposed ECoS solution.
    - Removal of support for Command Variants 2 and 3 (local delivery)
    - Updates to Response Code descriptions for existing Response Codes, E062302, E062303 and E062304 to support the proposed ECoS solution
    - New Response Codes and descriptions added for Response Codes, E062305, E062306 to support the proposed ECoS solution
- The Service Request Definition for SRV 8.13 *ReturnLocalCommandResponse (CoS)* in section 3.8.117 has been updated to reflect SRV 6.23 update to remove support for local delivery option.
- DCC Alert Messages in section 3.9 has been updated to add three (3) new DCC Alerts and associated definitions.
    - ECoSAlert (N63) and CoSCertificate Alert – N65 to support the proposed ECoS solution
    - CommsHubFirmwareActivation (N64) to support SEC Modification SECMP0024.
- Validation checks defined in section 3.10.2 have been updated for Response Code E1007 to extend the checks carried out to support the proposed ECoS solution for all Service Requests.
- The DUIS XML Schema contained within Annex A has been updated with a new v5.1 to include all of the additions and updates contained within the DUIS document and as detailed above.

Question 8	**Overall, do you agree with the proposed amendments to the DUIS (only those amendments that relate to ECoS) as outlined in this consultation? If you do not, please indicate any areas of disagreement and the reasons for them.**

4. Next Steps and Approval of the ECoS SEC Subsidiary Document Changes outlined in this consultation

Following the closure of this consultation, DCC will consider respondents' views. Subject to the consultation responses received, DCC will submit to BEIS, a summary of consultation responses received and any changes to the proposed amendments being consulted on in this document. DCC will provide the consultation summary to BEIS.

In addition, DCC will provide a summary to all stakeholders once we have discussed consultation responses with BEIS and determined next steps. This summary will be uploaded to the DCC website.

DCC has also discussed the designation of the SEC Subsidiary Documents being consulted on this consultation with BEIS. BEIS has indicated that it expects the documents (updated to reflect any changes in light of the consultation responses) will be designated at the time the ECoS service goes live – i.e. the point in time from which DCC can commence migration of devices to ECoS. BEIS will consult on the timing of this designation in due course.

The exception to the above is the ETMAD. The version of the ETMAD included within this consultation is planned to be designated by BEIS at the time that the main body SEC changes that are currently before Parliament are made. As outlined above, this is now expected to be in mid-October 2021, and for this reason DCC is seeking responses to the proposed changes to ETMAD by 13 October 2021 to feed into this process.

5. Summary list of consultation questions for respondents

As outlined in this consultation document, DCC would like stakeholders' views on the questions as they relate to the sections above. A summary of those questions are provided below for easy reference:

Q1	**ECoS User Testing** If you are a Supplier Party, do you intend to carry out testing of User Systems in order to verify that you are able to successfully submit 'Update Security Credentials (CoS)' Service Requests under the ECoS Arrangements and have them successfully processed?
Q2	**ECoS Transition and Migration Approach Document** Do you have any views on using the ETMAD to make a change to the SEC Section G obligations relating to the publication of the ECoS Interface Specification (i.e. that rather than DCC publishing the ECoS Interface Specification on the DCC website, requiring that it and any supporting Security Impact Assessments be made available to the DCC Independent Security Assessment Service Provider for review, as part of carrying out a DCC Security Assessment)? *Please note that we require any views in response to this question by 13 October 2021 so that those views can be considered by DCC and BEIS prior to the first version of the ETMAD taking effect in mid-October 2021.
Q3	**DCC User Interface Services Schedule (SEC Appendix E)** Do you have a view on whether the increased Target Response Times for 'Update Security Credentials (CoS)' Service Requests (Service Reference Variant

	(SRV) 6.23) will impact User operations? If you do consider there is an impact, please explain your rationale.
Q4	**DCC User Interface Services Schedule (SEC Appendix E)** Do you agree with the proposal to increase the Target Response Times 'Update Security Credentials (CoS)' Service Requests (Service Reference Variant (SRV) 6.23) from: • 30 seconds to 35 seconds where the Target Device is a SMETS2+ Device?; and • 16 seconds to 21 seconds where the Target Device is a SMETS1 Device? If you do not agree with this proposal, please indicate why.
Q5	**Threshold Anomaly Detection Procedures (SEC Appendix AA)** Overall, do you support the proposed amendment to the TADP as outlined in this consultation? If you do not, please indicate any areas of disagreement and reasons for them.
Q6	**Service Request Processing Document (SEC Appendix AB)** Overall, do you support the proposed amendments to the SRPD as outlined in this consultation? If you do not, please indicate any areas of disagreement and the reasons for them.
Q7	**Inventory Enrolment and Decommissioning Procedures (SEC Appendix AC)** Overall, do you support the proposed amendments to the IEDP as outlined in this consultation? If you do not, please indicate any areas of disagreement and the reasons for them.
Q8	**DCC User Interface Specification (SEC Appendix AD)** Overall, do you agree with the proposed amendments to the DUIS (only those amendments that relate to ECoS) as outlined in this consultation? If you do not please indicate any areas of disagreement and the reasons for them.

6. How to Respond

Please provide responses by **16:00 on 5 November 2021** to DCC at consultations@smartdcc.co.uk.

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. Please note that responses in their entirety (including any text marked as confidential) may be made available to BEIS and the Gas and Electricity Markets Authority (the Authority). 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.

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