Department for Business, Energy & Industrial Strategy

Department for Business, Energy & Industrial Strategy
1 Victoria Street
London SW1H 0ET
www.gov.uk/beis

The Authority (Ofgem), the SEC Panel, SEC Parties and other interested parties

1 April 2021

Dear Colleague,

SMART METERING IMPLEMENTATION PROGRAMME: CONSULTATION ON CHANGES TO THE SMART ENERGY CODE FOR THE ENDURING CHANGE OF SUPPLIER ARRANGEMENTS AND CERTAIN SECURITY PROVISIONS

This consultation seeks stakeholder views on the following:

- proposed changes to the Smart Energy Code (SEC) to support the introduction of the Enduring Change of Supplier Arrangements[1];
- an initial version of an ECoS Transition and Migration Approach Document (ETMAD), a new SEC Subsidiary Document planned to be used to control the process of transition and migration to ECoS, and the proposed date for its incorporation into the SEC;
- a number of further security-related changes to the SEC that affect the DCC, and one that applies to Users; and
- an update to the SMKI Interface Design Specification to support an alternative Certificate Signing Request process for Network Parties accessing the SMKI Portal via the Internet, and the proposed date for incorporating the revised document into the SEC.

The proposed SEC changes can be found in the Annexes to this letter. Subject to consideration of consultation responses and the Parliamentary process, the revised main-body SEC drafting will be introduced into the SEC using the Secretary of State's Section 88 Energy Act 2008 powers. We propose to introduce the first version of the ETMAD using the Secretary of State's powers under condition 22 of the DCC licence and Section X5 of the SEC to coincide with the main body changes being made using Section 88. We propose to make the changes to the SMKI Interface Design Specification also using condition 22/X5 powers shortly after this consultation closes.

[1] https://smartenergycodecompany.co.uk/latest-news/government-response-to-consultation-on-directing-the-dcc-to-plan-for-the-design-development-and-implementation-of-smart-metering-ecos-arrangements/

This consultation applies to the gas and electricity markets in Great Britain. Responsibility for energy markets in Northern Ireland lies with the Northern Ireland Executive's Department for the Economy.

Timing

Responses to this consultation should be submitted by 17:00 on 20 May 2021.

Responding to this consultation

Your response will be most useful if it is framed in direct response to the questions posed, by reference to our numbering, though further comments and evidence are also welcome.

Responses should be submitted to **smartmetering@beis.gov.uk** (given the situation with COVID-19, we are not accepting postal responses).

When responding, please state whether you are responding as an individual or representing the views of an organisation.

Confidentiality and data protection

Information you provide in response to this consultation, including personal information, may be disclosed in accordance with UK legislation (the Freedom of Information Act 2000, the Data Protection Act 2018 and the Environmental Information Regulations 2004).
If you want the information that you provide to be treated as confidential please tell us but be aware that we cannot guarantee confidentiality in all circumstances. An automatic confidentiality disclaimer generated by your IT system will not be regarded by us as a confidentiality request.

We will process your personal data in accordance with all applicable data protection laws. See our privacy policy.

We will summarise all responses and publish this summary on the SECAS website. The summary will include a list of organisations that responded, but not people's personal names, addresses or other contact details.

If you have any complaints about the way this consultation has been conducted, please email: beis.bru@beis.gov.uk.

Kind regards,

Duncan Stone
Deputy Director & Head of Delivery
Smart Metering Implementation Programme

List of Annexes and Attachments to this letter (the Attachments are separate documents)

Annex A	Consultation document
Attachment 1	Proposed legal drafting – Proposed changes to Section A
Attachment 2	Proposed legal drafting – Proposed changes to Section G
Attachment 3	Proposed legal drafting – Proposed changes to Section L
Attachment 4	Proposed legal drafting – Proposed initial version of ETMAD
Attachment 5	Proposed legal drafting – SMKI Interface Design Specification

Annex A: Consultation document

1. SEC Changes for the Enduring Change of Supplier Arrangements

Background

1.1. The DCC has commenced a programme of work to replace the existing Transitional Change of Supplier (TCoS) arrangements with a set of enduring arrangements – the Enduring Change of Supplier (ECoS) arrangements. This work is underpinned by a DCC plan[2] that has been established and approved by the Secretary of State under condition 13A of the DCC licence.

1.2. The essence of the changes to implement ECoS include:

- the procurement by DCC of a new External Service Provider to carry out the CoS Party role under the SEC in place of the existing TCoS service provider, this new provider being referred to in this document as the ECoS service provider;
- as compared to the existing arrangements, increased Separation between the CoS Party element of the DCC Live Systems from the access control broker functions[3] of DCC Live Systems, in line with BEIS's previous consultation on this issue[4];
- enhanced ECoS processes including, for example:
  - the use by suppliers of Private Keys associated with XML signing Certificates to Digitally Sign CoS Update Security Credentials Service Requests (Service Reference Variant (SRV) 6.23) whereby the link between registration data identifiers and EUI-64 identifiers of suppliers is cryptographically asserted and is then checked as part of CoS processing;
  - cessation of the sharing of Registration Data between DSP parts the DCC Live Systems (limb (a)) and the CoS Party, with a separate feed of Registration Data being provided directly to the CoS Party; and
  - enhanced anomaly detection arrangements;
- changes to the way in which CoS events are managed for SMETS1 Devices, such that under the enduring arrangements, the CoS Party will be involved in the processing of Service Reference Variant (SRV) 6.23 (CoS Update Security Credentials) Service Requests that relate to SMETS1 Devices and will need to cryptographically confirm that the CoS event is legitimate before it can be processed, by other parts of the DCC;
- the updating of Device Security Credentials on SMETS2+ Devices installed in consumer premises such that they are populated with information from a CoS Party Certificate that has been Issued to the ECoS service provider Systems rather than the TCoS service provider Systems. This will require a period of migration from TCoS to ECoS during which time, both the TCoS service provider and the ECoS service provider will needed to

---

[2] https://www.smartdcc.co.uk/media/3769/2-approval-of-plan-pursuant-to-condition-13a-of-smart-meter-communication-licence.pdf

[3] The access control broker systems of DCC are those that apply Anomaly Detection Thresholds, that Countersign SMETS1 Service Requests sent to SMETS1 Service Providers and that apply Message Authentication Codes to Commands to be sent to SMETS2+ Devices.

[4] https://smartenergycodecompany.co.uk/latest-news/24566/

process SRV 6.23s depending upon whether the Device Security Credentials of the target device are populated with information from a CoS Party Certificate held by the TCoS service provider or the ECoS Service Provider. Affected devices include ESME, GSME, GPF, HCALCS and SAPC. The TCoS service provider will need to Digitally Sign Commands to update Device Security Credentials such that target devices hold information from the ECoS service provider's Certificates rather than its own, i.e. to "Migrate" the Devices from TCoS to ECoS;

- management of the smart metering device supply chain, such that, from a point in time to be determined, newly installed devices may only be Commissioned if they have their Device Security Credentials populated from a CoS Party Certificate Issued to the ECoS service provider Systems and not the TCoS service provider Systems; and
- management of the interactions with the implementation of the Centralised Registration Service (also known as the Centralised Switching Service – CSS) which may require the ECoS service provider to interface with an interim solution for the provision of Registration Data.

1.3. Based on the plan for delivery of ECoS under condition 13A of the DCC licence (LC13A), the ECoS service is expected to go live in June 2022 from which time the replacement of the TCoS service provider's Certificate information in Device Security Credentials can commence and from which point in time the dual processing of SRV6.23s will be needed. Again, based on the LC13A plan, migration is expected to be complete by end April 2023, sometime after which, the TCoS systems will need to be decommissioned and the Certificates held by the TCoS service provider will need to be revoked.

1.4. Separately, BEIS has put in place a Baseline Margin Project Performance Adjustment Scheme (BMPPA Scheme) for the implementation of the ECoS Arrangements[5]. We are proposing to consult on further modifications to this scheme, in order to include additional measures relating to the processing of SRV6.23s in the migration period.

Approach to the Implementation of the SEC changes for ECoS

1.5. The introduction of the ECoS arrangements requires changes to the main body of the SEC as well as to several SEC subsidiary documents. BEIS is proposing to use its powers under Section 88 of the 2008 Energy Act to make the main body changes and to use powers under condition 22 of the DCC licence and section X5 of the SEC to make the SEC Subsidiary Document changes.

1.6. All of the SEC main body changes for the implementation of ECoS are being consulted on pursuant to the current consultation. They are summarised below and can be found in Attachments 1, 2 and 3.

ETMAD and changes to other SEC Subsidiary Documents highlighting potential User Impact

1.7. From an ECoS perspective, beyond the main body SEC changes, another key focus of this consultation is on an initial version of a new proposed SEC Subsidiary Document – the ECoS Transition and Migration Approach Document (ETMAD) at Attachment 4 to the letter. We are in discussions with DCC on it developing the necessary changes to other SEC Subsidiary

[5] https://smartenergycodecompany.co.uk/latest-news/beis-consultation-response-on-bmppa-scheme-for-ecos/

Documents in line with its LC13A Plan. Whilst we have a reasonable understanding of the likely changes that will be needed, DCC will want to wait until the detailed design for ECoS is completed before fully specifying them. We expect a further consultation on the "go-live" version of ETMAD expected Q4 2021, to apply from the commencement of migration.

1.8. With respect to other subsidiary documents, we are expecting changes to the Service Request Processing Document to explain the new processing of SRV6.23s under ECoS. In addition to requiring[6] that SRV6.23s are Digitally Signed with a Private Key associated with a Public Key that is contained within an XML signing Certificate[7], the way in which the DCC will carry out the Registration Data checks on these Service Requests will be different. The DCC will be required to use the registration data identifier[8] held within the XML signing Certificate that was used to check the digital signature on the Service Request to confirm that the Supplier Party who sent it is an incoming supplier for the relevant Device in the Registration Data. ***What this means is that if a Supplier Party has multiple registration data identifiers, it will need to select the "right" Private Key to Digitally Sign the Service Request in order for it to be successfully processed***. Here, the "right" Private Key means a Private Key that is associated with a Public Key that is contained within an XML signing Certificate that has an MPID in the Subject X520 Common Name that matches the specific MPID that is associated with the target device in Registration Data via the MPxN.

1.9. Suppliers can already elect to become subscribers for this type of Organisation Certificate[9] and can already use the associated Private Keys to sign Service Requests. The changes to the way in which the DCC applies the new Registration Data checks to SRV6.23s will not however apply until the commencement of ECoS Migration, planned for June 2022. Before these changes to DCC Systems are implemented (i.e. before the commencement of ECoS migration), BEIS will be looking for evidence that an adequate number of suppliers have successfully tested their ability to use these Private Keys and have SRV6.23 Service Requests successfully processed. ***Suppliers, and their Shared Resource Providers, are encouraged to engage with DCC and participate in testing their capability to do this as early as is practicable.***

Initial Version of ETMAD

1.10. Many of the main body SEC changes for ECoS upon which we are consulting are not needed until the commencement of ECoS Migration planned for June 2022. However, we plan to lay them before Parliament in July this year to ensure they are in place in good time. We propose to bring the changes into legal effect once the 40-day period in Parliament has ended (and subject to there being no Parliamentary objections to the changes). We propose to use ETMAD to initially undo those main body changes that are not needed until later. Doing so in

---

6 This change is being implemented through SEC Modification MP104 that will take effect at the same time as the commencement of ECoS Migration. We are in discussions with SECAS and DCC about the coordination of the changes that are planned for June 2022.

7 An "XML signing Certificate" in this context is an Organisation Certificate with a Remote Party Role that indicates that the associated Public Key will be used to sign XML.

8 Registration data identifiers are often referred to as "MPIDs" and this term is used subsequently in this document.

9 i.e. an Organisation Certificate that has a Remote Party Role of "xmlSign" and within which the Subject X520 Common Name is populated with one or two MPIDs.

this manner allows us more flexibility over when the changes are brought into effect, because we can control this by re-designating a new version of ETMAD.

1.11. The effect of the first version of ETMAD included within this consultation is essentially to undo the ECoS related main body SEC changes that should not be applied in Autumn 2021. Hence, we propose to incorporate the first version of ETMAD into the SEC at the same time that the main body ECoS changes are due to be brought into legal effect in Autumn 2021.

1.12. As part of the implementation of SEC Modification MP104, DCC is required to report, from November 2021, on whether or not Users are using Private Keys associated[10] with XML signing Certificates to sign Service Requests and Signed Pre-Commands. We wish to extend this reporting to understand whether Users are also using Private Keys associated with XML signing Certificates *with MPIDs in them* to sign SRV6.23 Service Requests. In order to underpin this reporting, we have proposed drafting in Clause 4 of the initial version of ETMAD.

1.13. Overall, therefore, the effect of the first version of ETMAD is only to undo the ECoS main body changes and to introduce an additional reporting obligation on DCC from November 2021. A second[11] version of ETMAD will be consulted upon and brought into effect for the commencement of ECoS migration currently planned for June 2022. This second version of ETMAD would:

- cease to undo the ECoS main body changes;
- set out the arrangements whereby SRV6.23s are processed differently by the DCC depending upon whether the target device holds Device Security Credentials that are ECoS related or TCoS related; and
- deal with other migration related matters.

1.14. Where there are any security affecting matters in the second (or subsequent versions) of ETMAD, we are requiring DCC to submit a security impact assessment on the changes to the Security Sub-Committee (SSC). Any observations on the security impact assessment from the SSC would need to be considered in finalising the document.

ECoS Interface Specification

1.15. The security of the CoS Party is a very important aspect of the overall security of Smart Metering and, as a consequence, we believe that the interface specification between the CoS Party and other DCC Systems needs to be subjected to a degree of scrutiny and change control that is not normally afforded to other internalised DCC interfaces. This ECoS Interface Specification document (or documents) will need to be developed by the DCC as part of its design processes for ECoS and shared with the relevant External Service Providers. We are proposing that the DCC should submit an initial draft of the document to the SSC in conjunction with a security impact assessment that sets out DCC's views on any impacts there may be on the End-to-End Security Architecture or the Security Risk Assessment. After considering any observations made by the SSC on the security impact assessment, and responding to the SSC, the DCC would then submit the interface specification to the Secretary

[10] More strictly, Private Keys associated with Public Keys contained within XML signing Certificates.

[11] We might make the changes to other SEC subsidiary documents (which we are planning to consult on in Q3 2021 before ECoS migration commences, in which case, there would need to be a further interim version of ETMAD to additionally undo these changes.

of State for approval and, following approval, publish the document on its website. Thereafter the DCC would need to submit any proposed revisions to the document to the SSC (again identifying any impacts there may be on the End-to-End Security Architecture or the Security Risk Assessment) and again consider any SSC observations on document before publishing the amended version.

1.16. We are not requiring explicit SSC approval of any subsequent changes but believe that requiring the DCC to publish the document and to consider SSC observations on DCC's security impact assessment of any changes before making them, will ensure that, where the documents are modified in the future, the importance of the security of the CoS Party interfaces will continue to be appropriately recognised.

Summary of proposed ECoS-related SEC Changes covered by this Consultation

1.17. The ECoS related SEC changes that are being proposed in this consultation are:

- a change to Section L to introduce a new type of Organisation Certificate for use by the (E)CoS Party[12] in conjunction with its signing of XML with a Remote Party Role of "coSPartyXmlSign";
- a change to sections G2.21 and G2.22E to reflect that under the ECoS Arrangements, the CoS Party will no longer be permitted to share access to Registration Data with the DSP[13];
- changes to Section G2 to require greater separation between the CoS Party Systems and the Access Control Broker Systems. BEIS consulted upon the underlying principles for these separation requirements in March 2020[14] and concluded in June 2020[15] and, as part of this consultation, we are now inviting views on the proposed legal drafting to give effect to these principles;
- additional provisions in Section G2.50 – G2.55 that deal with the initial approval and subsequent modification of the ECoS Interface Specification;
- a new Section G11 that deals with the scope, content and legal effect of the ETMAD;

[12] The "CoS Party" will continue to be referred to as the "CoS Party" in the main body SEC even though its operation will be underpinned by the ECoS systems rather than TCoS systems. The fact that during migration to ECoS, a second CoS Party (underpinned by TCoS Systems) will be operating in parallel with the CoS Party (underpinned by ECoS Systems), will be dealt with in the second version of ETMAD.

[13] In practice, the CoS Party will not have separate access to Registration Data until the Ofgem-led changes associated with the Centralised Registration Service arrangements are made. In the meantime, the CoS Party will continue to use DSP held Registration Data. The implementation of this "tactical solution" will be dealt with in the second version of ETMAD. We have agreed with Ofgem that, because the ECoS related SEC changes are being made before the Centralised Registration Service related SEC changes, the changes to Section E (Registration Data) that reflect that (in addition to the DSP) a separate feed of Registration Data will also be sent to the (E)CoS Party from the Centralised Registration Service systems, will be made as part of the Ofgem changes.

[14] https://smartenergycodecompany.co.uk/latest-news/beis-consultation-on-separation-of-ecos-systems-from-other-dcc-systems/

[15] https://smartenergycodecompany.co.uk/latest-news/24566/

- some minor consequential changes to Section A to reflect that the CoS Party will, under the ECoS Arrangements, be applying Anomaly Detection Thresholds[16]; and
- an initial version of ETMAD, in relation to which we propose to designate on 28 September 2021[17], or as soon as reasonably practicable within two months thereafter as the date for its initial incorporation into the SEC.

Consultation Questions	
1.	Do you have any comments on the proposed main body SEC changes for ECoS, or on the initially proposed version of ETMAD (which is intended to turn off the ECoS related SEC changes until the start of migration)?
2.	Do you agree with our proposal to designate the initial version of ETMAD for incorporation into the SEC on 28 September 2021, or as soon as reasonably practicable within two months thereafter?

[16] Please note that whilst we are generally undoing the ECoS related changes in the initial version of ETMAD until migration to ECoS commences, we have not proposed to undo these minor definitional changes, since we do not think it is necessary.

[17] Because, at the time of writing, the Parliamentary recess dates Summer 2021 have not yet been published, we are not sure if this is the precise date when the ECoS main body changes will take effect, the actual date is, we think, likely to be a few days after 28 September but well within the proposed 1 month leeway.

2. Further Security Related Changes

2.1. In developing the ECoS-related SEC changes, BEIS identified a number of other security-related changes that we believe it is appropriate to make to Section G of the SEC, which are contained within Attachment 2 to this letter. First, with the introduction of XML signing Certificates for Users in November 2020 and (under the ECoS Arrangements) for the CoS Party from June 2022, we are of the view that it would be appropriate also to make XML signing Certificates available to those other parts of DCC Systems that sign XML but which do not currently have access to such Certificates. This will allow DCC to avoid having to sign messages with Private Keys associated with Certificates that have GBCS Remote Party Roles and which could in theory be deployed on Devices.

2.2. The DCC Systems that sign XML include:

- the DSP systems – for signing Pre-Commands;
- the ACB systems – for countersigning SMETS1 Service Requests; and
- WAN Providers – for signing the equivalent of Service Requests and Signed Pre-Commands for communication with Devices.

2.3. We are, therefore, proposing three new types of XML signing Certificates for these DCC Systems[18] and propose changes to Section L to provide for these in addition to the XML signing Certificate for the CoS Party.

2.4. Next, we also proposing two corrections to L3.18, first to clarify that Issuing Authority OCA Certificates are Issued to limb (d) of DCC Live Systems, and second to clarify that Certificates with a Remote Party Role of "accessControlBroker" are issued to either limb (a) or limb (b) of DCC Live Systems depending upon whether the key usage of the Certificate is digital signature or key agreement. Limb (a) of DCC Live Systems uses the Private Key associated with a "digital signing" Certificate to digitally sign commands, for example those used to join PPMIDs to other Devices, and limb (b) of DCC Live Systems uses the key agreement key to calculate message authentication codes.

2.5. We are also proposing measures to require DCC to begin using these new Certificate types and associated Private Keys, but in a manner that is designed not to lead to any material costs for DCC. Specifically, we are proposing (in G2.56 to G2.61) the following changes:

- where Private Keys are used by the DCC to create signatures on Commands sent to devices, the DCC should only use those keys for that purpose (or for signing a Certificate Signing Request in the first instance). Our understanding is that DCC's service providers already meet this requirement;
- where:

[18] Certificates are Issued to various parts of DCC Live Systems. Both the WAN Provider and the majority of the DSP Systems (excluding, for example, the Access Control Broker Systems) fall within limb (a) of the definition of DCC Live Systems because there is no requirement for these Systems to be Separate under the SEC. Two of the new XML signing Certificates are therefore available to the same part of DCC Live Systems. In practice, however we are expecting one of these types of Certificate to be used to check WAN Provider signatures and the other to check DSP signatures.

- the DCC has a Private Key that is associated with a Certificate with a Remote Party Role that is set out in GBCS (rather than Annex 1 to Section L of the SEC) – so for example “accessControlBroker” or “wanProvider”, and
- the DCC uses that Private Key for non-GBCS related actions (e.g. for signing XML or file signing), then
- the DCC must (where reasonably possible at the earliest opportunity[19], and in any event no later than when the current Certificate expires), replace the Private Key with one that is associated with an XML signing Certificate;

- from no later than the ECoS Service Live date (as set out in the LC13A plan, i.e. currently planned for June 2022), the DCC must no longer become a subscriber for a new Certificate with a Remote Party Role defined in GBCS if the associated Private Key is going to be used for purposes other than those described in GBCS (e.g. if it is to be used for XML signing or file signing). There is an exception if this becomes necessary following a recovery event. The backstop date for this obligation is to allow DCC time to reach a position that it is able to meet the obligation, to the extent that it needs time to be able to do so; and
- the DCC must ensure that the Root OCA Private Key and Issuing OCA Private Keys are only used for the purposes for which they are intended (signing OCA Certificates or Organisation Certificates, signing CSRs and signing Authority Revocation Lists (ARLs) or Certificate Revocation Lists (CRLs)). We understand that DCC is already doing this but think that it is helpful to set out this restriction for future reference.

2.6. In addition, we are also proposing an obligation on Users in G3.29 to require them to ensure that where they use a Private Key to create signatures that form part of Commands sent to Devices, they do not also use that Private Key for other purposes (again with the exception of signing a Certificate Signing Request to be Issued with the associated Organisation Certificate in the first instance). This obligation is linked to (but slightly different from) the obligations Users already face under Paragraph 3.3.1 of the DCC User Interface Specification (SEC Appendix AD) which requires that Private Keys used to sign XML (i.e. Service Requests and Signed Pre-Commands) are different from those used to sign GBCS Payloads held within Signed Pre-Commands.

2.7. Finally, we are proposing to strengthen the obligations placed on DCC in relation to its management of updates to its global Anomaly Detection Thresholds (ADTs). In G6.6A, we are proposing that where one part of DCC sends updated thresholds to another part of DCC (i.e. to the Access Control Broker and, under the future ECoS Arrangements, to the CoS Party), the recipient system must check the cryptographic protection on the updated ADT file and apply anti-replay checks. Again, to give DCC time to implement these changes, we are requiring that they must be implemented by no later than the ECoS Service Live date.

Consultation Question

3.	Do you have any comments on the proposed changes to Section G described in this section?

[19] By this we are intending that the DCC should not incur excessive costs in order to replace the Certificates at an early stage however should do so if opportunity allows.

3. Changes to the SMKI Interface Design Specification

3.1. On 3 March 2021, the Chair of the SMKI PMA wrote to BEIS asking it to use its powers under condition 22 of the DCC licence and X5 of the SEC to expedite changes to the SMKI Interface Design Specification (SMKI IDS) relating to the process by which Network Parties who are Authorised Subscribers using the SMKI Portal over the Internet ("SPOTI") service could submit Certificate Signing Requests (CSRs) for Organisation Certificates.

3.2. A number of Network Parties are seeking a lower cost mechanism for submitting CSRs over the SPOTI service. In particular the proposed alternative allows Network Parties to exclude the User EUI-64 Identifier for in the initial CSR submission and for this to be submitted at a later stage in the process in hexadecimal format (following a check by a member of the Registration Authority to confirm that the EUI-64 Identifier is one that has been allocated to the Authorised Subscriber).

3.3. The proposed changes to the SMKI IDS to accommodate this (which implicitly only require DCC to provide the alternative service once its systems have been tested and are ready to do so) are set out in Attachment 5 to this letter.

3.4. Subject to considering any comments received, BEIS proposes to re-designate on 2 June 2021, or as soon as reasonably practicable within 1 month thereafter, this revised version of the SMKI IDS into the SEC.

Consultation Questions	
4.	Do you have any comments on the proposed changes to the SMKI IDS?
5.	Do you agree with the proposal to re-designate the SMKI IDS for incorporation into the SEC on 2 June 2021, or as soon as reasonably practicable within 1 month thereafter?