Data Communications Company

SMETS1 Consultation on the SMETS1 Cryptographic Key Management Policy

A DCC consultation on the SMETS1 Cryptographic Key Management Policy

Date: 22 October 2021
Author: consultations@smartdcc.co.uk
Classification: DCC Public

Table of Contents

1. Introduction and Context

In the initial stages of the smart meter roll-out across Great Britain, a number of energy suppliers installed first generation smart devices (known as SMETS1 devices), in consumers' premises. SMETS1 devices installed by one energy supplier, however, are not always interoperable with and supported by the systems used by another supplier. The Data Communications Company (DCC) has developed a plan and designed a solution for the incorporation of such devices into its national network. It provides important shared benefits for industry and consumers and intends to offer the ability for SMETS1 consumers to maintain their smart services following a decision to switch suppliers.

SEC Section L of the Smart Energy Code (SEC) sets out the arrangements that govern the Smart Metering Key Infrastructure (SMKI) which underpins the security of smart-meter related communications. In order to provide governance of the SMKI documentation and gain assurance of the DCC operation of the SMKI Services, the SMKI Policy Management Authority (SMKI PMA) was established under the SEC and serves as a Sub-Committee of the SEC Panel.

Section L14.7 requires DCC to develop a SMETS1 Cryptographic Key Management Policy. Pursuant to this requirement, DCC has developed a SMETS1 Cryptographic Key Management Policy, which it has shared with the SMKI PMA. The SMKI PMA has reviewed the content of the document and provided comments which DCC has addressed. The SMKI PMA are satisfied with the content of the document and DCC is now seeking to have the SMETS1 Cryptographic Key Management Policy incorporated into the SEC.

Pursuant to Section L14.8 of the SEC, DCC is consulting on the draft content of the SMETS1 Cryptographic Key Management Policy for DLMS Devices and is seeking views on the proposed content of the policy.

2. SMETS1 Cryptographic Key Management Policy

For SMETS1 meters that use DLMS, commands sent to the meters are secured by separate keys for encryption and for authentication.

Section 20 of the SMETS1 Supporting Requirements (S1SR) places an obligation on DCC to ensure that for the SMETS1 Communications Hub Function or a SMETS1 Smart Meter or a SMETS1 Gas Proxy Function or a SMETS1 PPMID, the DCO will re-generate and replace any Authentication Keys and any Encryption Keys for any such supported Device. This process is required to occur seven days after commissioning following enrolment of the device on the DCC System and then every 15 months thereafter.

A SMKI PMA working group reviewed this obligation and recommended that a policy should be drafted for periodic SMETS1 symmetric key rotation such that, subject to meeting SMETS1 post commissioning obligations on key rotation following enrolment, the defined SMETS1 symmetric keys should not be subject to a 15 month (or any other period) periodic rotation.

The SMKI PMA considered the risks related to symmetric key rotation and could not identify any residual risk where either extant Section G controls did not already mitigate risk to well within tolerance or where the periodic rotation of symmetric keys, would be an effective control.

The proposed SMETS1 Cryptographic Key Management Policy which DCC is consulting on provides the framework for the periodic rotation of symmetric keys in accordance with Section 14.7.

Section 20 of the S1SR sets out the requirement to rotate keys on a 15-month basis and DCC is proposing to remove this obligation from the S1SR due to the changes that will be introduced by the proposed SMETS1 Cryptographic Key Management Policy.

CKMP Q1	Do you agree with the proposed approach to the rotation of symmetric keys? Please provide rationale for your reasoning.

2.1. Proposed SMETS1 Cryptographic Key Management Policy

DCC is proposing the addition of a new appendix to the SEC, the SMETS1 Cryptographic Key Management Policy for DLMS Devices. The policy document provides for the approach outlined in this consultation documents as well as meeting the obligation to produce such a document as set out in Section L14.7 of the SEC.

CKMP Q2	Do you have any comments on the proposed SMETS1 Cryptographic Key Management Policy for DLMS Devices?

2.2. Proposed Changes to the main body SEC

DCC is proposing a minor change to the main body of the SEC which is required as a consequence of the inclusion of the SMETS1 Cryptographic Key Management Policy for SMETS1 DLMS Devices into the SEC.

DCC is proposing to change the definition of SMETS1 Cryptographic Key Management Policy in Section A (definitions and Interpretation) as follows:

means any SEC Subsidiary Document of that name set out in Appendix [AT~~TBC~~], which is originally to be developed pursuant to Section L14.7 (The SMETS1 Cryptographic Key Management Policy: Document Development) and Section L14.8 (Document Development: Process).

CKMP Q3	Do you have any comments on the proposed consequential change to the main body of the SEC within the scope of this consultation?

2.3. Proposed Changes to the S1SR

DCC is proposing a change to the S1SR to remove the obligation in Section 20 to rotate symmetric keys every 15 months. The change would be the following:

As soon as reasonably practicable (and in any event within 7 days) following the Commissioning of a SMETS1 Communications Hub Function or a SMETS1 Smart Meter or a SMETS1 Gas Proxy Function or a SMETS1 PPMID ~~and at intervals no greater than 15 months thereafter~~, the S1SP shall, via the DCO, in relation to each such Device and where supported by that Device, re-generate and replace any Authentication Keys and any Encryption Keys (with their DLMS COSEM meanings) held by that Device.

CKMP Q4	Do you have any comments on the proposed drafting change to the SMETS1 Supporting Requirements document within the scope of this consultation?

3. Next Steps

Following the closure of this consultation, DCC will consider respondents' views, and, subject to the consultation responses received, submit to the Department for Business, Energy and Industrial Strategy a version of the proposed SMETS1 Cryptographic Key Management Policy and the proposed changes to the SEC that it considers suitable for re-designation into the SEC by the Secretary of State.

DCC is aiming to provide these documents to BEIS by 26 November 2021. DCC has discussed the designation of proposed SMETS1 Cryptographic Key Management Policy, re-designation of the S1SR with BEIS and it is proposed that, subject to timely receipt of DCC's report and copies of relevant stakeholder responses to this consultation, BEIS will make these changes on 10 December 2021 or as soon as reasonably practicable within one month thereafter.

In order to expedite these changes to the SEC, DCC is also seeking views on behalf of BEIS on the proposed date for designation and re-designation as well as the draft direction which is presented in Attachment 1 of this consultation document for stakeholder consideration.

CKMP Q5	Do you have any comments on the draft direction included in Attachment 1 or on the proposed date of 10 December 2021 or as soon as reasonably practicable within one month thereafter for designation of the proposed SMETS1 Cryptographic Key Management Policy and the redesignation of the S1SR?

4. How to Respond

Please provide responses by 1600 on 19 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 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 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 Information 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.

5. Attachments

- Attachment 1: Draft Direction
- Attachment 2: SMETS1 Cryptographic Key Management Policy
- Attachment 3: SMETS1 Supporting Requirements

- Attachment 4: Change to Section A – Definitions and Interpretation
- Attachment 5: Response template

Attachment 1

This attachment contains the text that BEIS plans to use for direction related to the SMETS1 Cryptographic Key Management Policy and the S1SR.

<u>Draft Direction Text</u>

This direction is made for the purposes of the smart meter communication licences granted under the Electricity Act 1989 and the Gas Act 1986 (such licences being the "DCC Licence") and the Smart Energy Code designated by the Secretary of State pursuant to the DCC Licence (such code being the "SEC").

Words and expressions used in this direction shall be interpreted in accordance with Section A (Definitions and Interpretation) of the SEC.

Pursuant to Condition 22 of the DCC Licence and Section X5 (Incorporation of Certain Documents into this Code) of the SEC, the Secretary of State directs that, with effect from [DD MM YYYY]:

i) *the SMETS1 Cryptographic Key Management Policy will be designated and incorporated in the form set out in Annex [XX] to this direction as SEC Appendix AT;*

ii) *the SMETS1 Supporting Requirements previously designated and incorporated into the SEC as Appendix AM is hereby re-designated and incorporated in the form set out in Annex [YY] to this direction;*

iii) the Smart Energy Code contents shall be updated to additionally include the following words at the end of the list of Appendices:

“Appendix AT: SMETS1 Cryptographic Key Management Policy”

iv) and the following definition shall be included (in alphabetical order) in Section A of the SEC:

SMETS1 Cryptographic Key Management Policy	**means the SEC Subsidiary Document set out in Appendix AT**

For the avoidance of doubt such re-designation of the SMETS1 Supporting Requirements shall be without prejudice to anything done under the DCC Licence or the SEC on or after this document first being designated, or to the continuing effectiveness of anything done this document prior to its re-designation (which shall have effect as if done under the re-designated document).

This direction is also being notified to the SEC Administrator.