Data Communications Company

SMETS1 Consultation on the SMETS1 MOC Public Key Infrastructure (PKI)

DCC Conclusions and Report to Secretary of State

Date: 4 September 2020
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.

Section L of the 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.

Depending on the SMETS1 Service Provider (S1SP), communications to SMETS1 devices from S1SPs are secured using either a dedicated, non SMKI PKI or by using symmetric keys. BEIS introduced changes that aligned the management of these S1SP PKIs and the symmetric keys under the aegis of the SMKI Policy Management Authority (SMKI PMA) and required the incorporation of relevant documentation into the SEC. This was to ensure a consistent set of oversight arrangements on the management of keys that are used as part of the secure end-to-end communication for SMETS1.

For the Secure S1SP, DCC is proposing to use a separate PKI to the existing version in the SEC for secure communication between devices and the MOC S1SP and DCO. As the PKI is an essential element of the end-to-end security of communications with their associated SMETS1 devices, BEIS placed this under the oversight of the SMKI PMA to provide a consistent set of oversight arrangements with SMKI. The result is that the certificate policies for the MOC PKI would, on incorporation into the SEC, need to be reviewed by the SMKI PMA in the same way that applies to the SMKI documentation. Both the Certificate Policy for Secure and the S1SPKI Compliance Policy had already been reviewed and approved by the SMKI PMA prior to publication of the consultation.

Pursuant to Section L of the SEC, DCC consulted on an equivalent of the SMKI compliance policy that applies to the additional SMETS1 MOC. DCC sought views on the SMETS1 PKI for MOC Secure suite of documents which consists of the S1SPKM Compliance Policy, and the MOC, Secure S1SPKI Certificate Policy.

2. Consultation

On 17 July DCC consulted on the content of the PKI for MOC. The consultation closed on 14 August 2020. In the consultation DCC sought views on a proposed SMETS1 Service Provider Key Management (S1SPKM) Compliance Policy and S1SP Certification Policy for MOC Secure.

This document considers responses to this consultation consistent with the regulatory requirements in Section L14.8 of the SEC which provides for the Document Development Process.

DCC also sought views on behalf of BEIS on the proposed date for designation of the SISPKI Compliance Policy and Certificate Policy for Secure as well as the draft direction which was presented in Attachment 1 of the consultation document.

DCC sought comments on the following questions:

Number	Question
PKI Question 1	Do you have any comments on the S1SPKM Compliance Policy?
PKI Question 2	Do you have any comments on the S1SPKI Certificate Policy for Secure?
PKI Question 3	Do you agree with the proposed designation date of 11 September 2020, or as soon as reasonably practicable within 1 month thereafter for both the SISPKI Compliance Policy and Certificate Policy for Secure?

Table 1

2.1. Respondents

DCC received four responses to the consultation.

3. Analysis of Responses

DCC has undertaken an analysis of the feedback provided by each respondent regarding the SISPKI Compliance Policy and Certificate Policy for Secure which is presented within this section document.

3.1. Comments relating to question 1

One respondent agreed with the proposals and requirements but made a comment on section 3 of the S1SPKM policy document. The respondent recognises the range of obligations placed on the DCC to confirm the financial rights and interests associated with a prospective independent provider ahead of contractual terms being agreed. However, they note that section 3 makes no reference to the independence of the individual assessors who would undertake the fieldwork. The respondent requests confirmation that the DCC will have to assure itself, and provide evidence, of assessor independence to a level equivalent to the requirements specified in SEC Section G2.23 and G2.24.

DCC response:

DCC can confirm that it has procured the provision of Independent Assurance Services for the assessment of the S1SPKI Services which satisfies the suitability and independence requirements specified in Section 3 of the S1SPKM Compliance Policy and SEC Section G. The assessors procured are recognised by the UK's National Accreditation Body (UKAS) responsible for determining the technical competence and integrity of organisations and their services.

3.2. Comments relating to question 2

All four respondents had no additional comments on the S1SPKI Certificate Policy for Secure.

3.3. Comments relating to question 3

All four respondents agreed with proposed designation date for both the SISPKI Compliance Policy and Certificate Policy for Secure.

4. Summary of Changes to the SISPKI Compliance Policy and Certificate Policy for Secure

In light of the consultation responses received, DCC is not proposing any changes to the SISPKI Compliance Policy and Certificate Policy for Secure.

5. Conclusions

DCC is of the opinion that the version of the SISPKI Compliance Policy and Certificate Policy, which will be submitted to the Secretary of State reflects the requirements set out in Section L14 of the SEC.

DCC is of the opinion that the SISPKI Compliance Policy and Certificate Policy for Secure is fit for purpose in that it meets the requirements set out in Section L14 of the SEC by clearly and unambiguously setting out parties' rights and obligations.

DCC is of the opinion that it has had appropriate consultation with industry regarding the content of the SISPKI Compliance Policy and Certificate Policy for Secure. DCC has, where necessary, addressed the comments that have been received from industry and it is accordingly DCC's view that it has met its SEC obligation set out in Section L14 of the SEC.

6. Next Steps

DCC will submit the updated version of SISPKI Compliance Policy and Certificate Policy for Secure that includes the changes identified in Section 4 of this document to the Secretary of State on 4 September 2020.

DCC anticipates that the Secretary of State will designate the SISPKI Compliance Policy and Certificate Policy for Secure into the SEC using its Section X powers on or shortly after 11 September 2020.

7. Attachments

- Attachment 1 – S1SPKM Compliance Policy
- Attachment 2 – S1SPKI Certificate Policy for Secure