



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

14 May 2019

Dear Colleague,

**Government response to March 2019 consultation on proposed amendments to the Smart Energy Code related to the contents of the SMETS1 Pending Product Combinations list and Cryptographic Processing in respect of SMETS1 Devices**

1. On 26 March 2019 we published a consultation seeking stakeholder views on proposed amendments to Section G of the Smart Energy Code (SEC) related to Cryptographic Processing in respect of SMETS1 Devices, and to Section F of the SEC in relation to the contents of the SMETS1 Pending Product Combinations list.
2. The consultation closed on 16 April 2019 and we received a total of 7 written responses from the following organisations:

Organisation type	Respondents
Energy suppliers	British Gas E.ON EDF Energy Npower SSE
Other organisations	DCC Energy UK

3. During the consultation period a number of bilateral meetings were held with individual stakeholders, including the DCC, the National Cyber Security Centre (NCSC), in addition to engagement through the SEC Panel Security Sub-Committee (SSC).
4. This document sets out the Government response to the consultation. Every effort has been made to ensure that the explanatory text in the main body of this Government response reflects the legal drafting in Annexes A and B. The legal drafting should be considered to be definitive in the event that there is an inconsistency between it and the explanatory text. Where terms defined in the SEC (or in licence conditions) are used in this Government response document, they are capitalised.

## Question 1: Proposed Section G amendments

### Issue under consideration

5. The DCC identified that Section G2.44 of the SEC, which describes how Cryptographic Processing is carried out in respect of both SMETS1 and SMETS2 Devices, would require amendment to enable SMETS1 Devices to be operated without requiring substantial changes to systems and devices (which would, in turn, have significant consequential impacts on the costs and timescales for delivering enrolment).
6. BEIS therefore proposed to modify Section G2.44 of the SEC such that the requirement to ensure that Cryptographic Processing is carried out within Cryptographic Modules which are compliant with the FIPS 140-2 Level 3 standard only applies in relation to DCC communications with SMETS1 Devices where:
  - a) The Cryptographic Processing is carried out by a DCO and involves the use of a SMETS1 Symmetric Key.
  - b) The Cryptographic Processing involves the use of a DCC Private Key to establish Transport Layer Security (TLS) in order to communicate with a SMETS1 Device;
  - c) The Cryptographic Processing involves the use of a SMETS1 Symmetric Key and is carried out by a SMETS1 Service Provider, except where:
    - i. the Cryptographic Processing is carried out to generate a Command to “add credit” to a SMETS1 Device;
    - ii. the SMETS1 Symmetric Key is used to generate an Instruction to a target Device that is identified as a Category 1 Device in the SMETS1 Supporting Requirements document;
    - iii. the SMETS1 Symmetric Key is only valid for the duration of a single Application Association and the target Device is identified as a Category 2 Device in the SMETS1 Supporting Requirements document; or
  - d) Any use of a Symmetric Key by a SMETS1 Service Provider that is (1) required to establish a session for Transport Layer Security with a SMETS1 Device, (2) is generated as part of the establishment of the session, and (3) is destroyed at the termination of that same session.<sup>1</sup>
7. We additionally proposed to modify Section G2.45 of the SEC such that all Cryptographic Processing that does not fall within the scope of Section G2.44 will need to be carried out within Cryptographic Modules established in accordance with the DCC’s Information Classification Scheme.
8. Consequential amendments to Section A of the SEC were also proposed.

### Summary of responses

9. Of the seven stakeholders who responded to this question, five agreed with the proposed changes while one energy supplier disagreed and a further energy supplier neither agreed nor disagreed. The respondent that disagreed with the proposed changes did so on the grounds that they considered themselves unable to comment on the proposals prior to

---

<sup>1</sup> This element has been added on the basis of consultation discussions; see below.

receiving confirmation from the NCSC that they are appropriate from a cryptographic communications perspective. They also raised concerns around the security implications of having consulted upon the proposed changes with all SEC Parties.

### Government response

10. In reaching our conclusions on the proposed changes we have considered the written responses to our consultation, our wider engagement with stakeholders, and the views of NCSC and the SEC Panel Security Sub-Committee. This resulted in addition of extra text in 6(d) above to account for DCC's approach to the implementation of Transport Layer Security for SMETS1 Service Providers.
11. We consider the changes outlined for Section G of the SEC as updated to be an appropriate and proportionate use of cryptography for communications to SMETS1 Devices. We note that the circumstances under which Cryptographic Processing needs to be carried out within Cryptographic Modules which are compliant with the FIPS 140-2 Level 3 standard (or equivalent) are already set out in Section G, and we are simply seeking to amend the existing requirements to ensure that appropriate provision is made ahead of the enrolment of SMETS1 meters in the DCC. Any amendments to Section G of the SEC will always need to be made following appropriate consultation with stakeholders. We engaged with NCSC prior to publication of this consultation.

### Conclusions

12. Following consideration of stakeholder responses and having engaged NCSC and the SEC Panel Security Sub-Committee, we have concluded that the proposed amendments to Section G of the SEC as updated are appropriate.

## **Question 2: Proposed Section F amendments**

### Issue under consideration

13. In June 2018 we concluded<sup>2</sup>, following consultation with stakeholders, that the DCC should be required to maintain, and provide to the Panel for publication, a list of the SMETS1 Device Model combinations in relation to which it is developing and/or testing its ability to successfully process SMETS1 Service Requests and relevant SMETS1 Alerts. This list is known as the SMETS1 Pending Product Combinations.
14. We additionally concluded that, as a result of the conflicting views expressed by stakeholders, further consideration was required in relation to the information that may be shared publicly about devices that are undertaking or have failed to complete SMETS1 Pending Product Combination Tests. We consequently asked the DCC to consider this matter further and propose any associated rules or procedures for inclusion in the Enduring Testing Approach Document. The DCC subsequently consulted and concluded upon a provision in the Enduring Testing Approach Document (clause 9.3), re-designated by BEIS on 13 March 2019<sup>3</sup>, which requires the DCC to not add a Device Model combination to the

---

<sup>2</sup> See: <https://smartenergycodecompany.co.uk/latest-news/government-response-to-the-march-2018-consultation-on-regulatory-changes-to-enable-provision-of-a-smets1-service-by-the-dcc/>

<sup>3</sup> See: <https://smartenergycodecompany.co.uk/latest-news/sec-version-6-9-designated/>

SMETS1 Pending Product Combinations where it has been informed by the relevant Testing Participant that the Manufacturer name is to be kept confidential.

15. In our March 2019 consultation we therefore proposed to make a consequential change to Section F2.10A of the SEC to clarify that the DCC should not add a Device Model combination to the SMETS1 Pending Product Combinations where the relevant Testing Participant has indicated, pursuant to clause 9 of the Enduring Testing Approach Document, that such information should be treated as confidential.

#### Summary of responses

16. Of the seven stakeholders who responded to this question, five agreed with the proposed change while two energy suppliers neither agreed nor disagreed. Further clarification was requested by respondents in relation to the following points:
  - a) The rationale for enabling a Meter Manufacturer's identity to be kept confidential during testing, and the circumstances under which a request for confidentiality will be upheld;
  - b) The visibility of Device Model combinations being tested, and how BEIS and DCC intend to balance the need for confidentiality against the need for transparency for other interested Parties (for example, a supplier that has become responsible for a meter following change of supplier);
  - c) Possible interactions between the proposed Section F drafting and requirements under Sections G3.17 and G3.18 of the SEC relating to the notification of material security vulnerabilities to the SSC; and
  - d) The responsibility for adding the resulting Device Model combination to the PPC when a new firmware version is released by a Meter Manufacturer.

#### Government response

17. Clause 9.3 of the ETAD states that a supplier must ensure that it has obtained consent from any relevant Manufacturer for its name to be published to the SMETS1 Pending Product Combinations list. Where a supplier is unable to obtain this consent, it must notify the DCC that the information is to be treated as confidential and the DCC will not add the relevant Device Model combination(s) to the SMETS1 Pending Product Combinations list. These requirements have been incorporated into the SEC following consultation on the draft ETAD by the DCC and as a result of concerns raised by a number of energy suppliers in relation to the potential for this information to be commercially sensitive.
18. While we recognise that a number of energy suppliers consider that this information may need to be kept confidential under certain circumstances while undertaking SMETS1 Pending Product Combination Testing (PPCT), we also recognise that suppliers require visibility of the Device Model combinations being tested against during Systems Integration Testing (SIT) and Device Model Combination Testing (DMCT) in order to prepare for enrolment of SMETS1 Smart Metering Systems. For that reason (among others), the DCC is required to discuss its Device Model selection for SIT with stakeholders and to subsequently notify Supplier Parties of its decision. We consider that a similar level of transparency will be required during DMCT, and expect this to be reflected in DCC's proposed amendments to the SMETS1 SEC Variation Testing Approach Document (SVTAD) to enable DMCT when it is published for consultation. Where a Supplier wishes to obtain visibility of a Device Model combination in respect of which PPCT is being

undertaken subject to the confidentiality provisions set out in ETAD, we would encourage that Supplier to contact the relevant Manufacturer.

19. We do not consider that there is any interaction between the proposed Section F drafting and the requirements of Sections G3.17 and G3.18 of the SEC relating to the notification of material security vulnerabilities to the SSC, which apply (and will continue to apply) in respect of all Enrolled Smart Metering Systems. Even where an energy supplier notifies the DCC that it has not obtained consent for a Device Model combination to be listed on the SMETS1 Pending Product Combinations, we would note that the Device Model combination in question will nonetheless be added to the SMETS1 Eligible Product Combinations following successful completion of any required testing.
20. Section H5.9 of the SEC states that the DCC is only required to process Service Requests in respect of SMETS1 Smart Metering Systems that comprise a combination of Device Models that is listed on the SMETS1 Eligible Product Combinations. Where a Supplier wishes to apply a firmware upgrade to a device due to a new Manufacturer release, this will result in a new Device Model combination. Consequently, where an energy supplier wishes to benefit from the obligation on DCC in Section H5.9 described above, it should seek to put the new Device Model combination through PPCT prior to deploying the firmware upgrade, as this is the route to getting the Device Model combination onto the list of SMETS1 Eligible Product Combinations. We note that the decision on whether to move to a new firmware version post-enrolment is one to be taken by the responsible supplier in all cases. This will enable any end-to-end testing that is required to be carried out, and firmware deployments to be planned according to suppliers' individual needs and business processes. DCC have been asked to consider how the arrangements should work where firmware needs to be deployed immediately (for example, due to a security vulnerability) and the DCC has informed us that it will be consulting on proposed amendments to the ETAD to cater for this in the near future.

### Conclusions

21. Following consideration of stakeholder responses, we have concluded that the proposed amendment to Section F of the SEC is appropriate.

### **Implementation of conclusions**

22. We intend to lay the legal text set out in Annexes A and B before Parliament on 14 May 2019, in line with the procedure under Section 89 of the Energy Act 2008. Subject to no objection being raised during the 40-day laying period, we expect to bring the relevant modifications to the main body of the SEC into effect in July 2019.

Kind regards,



**Duncan Stone**

Head of Delivery

Smart Metering Implementation Programme

### List of Annexes to this letter

<b>Annex A</b>	Legal text of amendments to Sections G & A of the SEC
<b>Annex B</b>	Legal text of amendments to Section F of the SEC