

This document is classified as **Clear** in accordance with the Panel Information Policy. Recipients can distribute this information to the world, there is no limit on disclosure. Information may be shared without restriction subject to copyright.

MP268 ‘Certificate rotation and expired Certificates’

Annex B

Legal text – version 1.0

About this document

This document contains the redlined changes to the SEC that would be required to deliver this Modification Proposal.

Section G ‘Security’

These changes have been redlined against Section G version 23.0.

Amend Section G.8.3 as follows:

G8. USER SECURITY ASSURANCE

Scope of Security Assurance Services

G8.3 The security assurance services specified in this Section G8.3 are services in accordance with which the User Independent Security Assurance Service Provider shall:

- (a) carry out User Security Assessments at such times and in such manner as is provided for in this Section G8;
- (b) produce User Security Assessment Reports in relation to Users that have been the subject of a User Security Assessment;
- (c) receive and consider User Security Assessment Responses and carry out any Follow-up Security Assessments at the request of the Security Sub-Committee;
- (d) otherwise, at the request of, and to an extent determined by, the Security Sub- Committee, carry out an assessment of the compliance of any User with its obligations under Sections G3 to G6 where:
 - (i) following either a User Security Self-Assessment or Verification User Security Assessment, any material increase in the security risk relating to that User has been identified; or
 - (ii) the Security Sub-Committee otherwise considers it appropriate for that assessment to be carried out;
- (e) review the outcome of User Security Self-Assessments;
- (f) at the request of the Security Sub-Committee, provide to it advice in relation to:
 - (i) the compliance of any User with its obligations under Sections G3 to G6 or any CPA Certificate Remedial Plan;
 - ~~(ii)~~ changes in security risks relating to the Systems, Data, functionality and processes of any User which fall within Section G5.14 (Information Security: Obligations on Users); and
 - ~~(ii)(iii)~~ the compliance of any User with obligations under SEC Appendix AC Section 5.22 and SEC Appendix AC Section 5.23;
- (g) at the request of the Panel, provide to it advice in relation to the suitability of any remedial action plan for the purposes of Section M8.4 of the Code (Consequences of an Event of Default);

- (h) at the request of the Security Sub-Committee Chair, provide a representative to attend and contribute to the discussion at any meeting of the Security Sub-Committee; and
- (i) undertake such other activities, and do so at such times and in such manner, as may be further provided for in this Section G8.

Amend Section G9.2 as follows:

G9. DCC SECURITY ASSURANCE

Scope of Security Assessment Services

G9.2 The security assessment services specified in this Section G9.2 are services in accordance with which the DCC Independent Security Assessment Service Provider shall:

- (a) carry out DCC Security Assessments at such times and in such manner as is provided for in this Section G9;
- (b) produce DCC Security Assessment Reports in relation to the DCC that have been the subject of a DCC Security Assessment;
- (c) receive, consider and validate DCC Security Assessment Responses and carry out any Follow-up Security Assessments at the request of the Security Sub-Committee;
- (d) otherwise, at the request of, and to an extent determined by, the Security Sub Committee, carry out an assessment of the compliance of the DCC with its obligations under:
 - (i) Condition 8 (Security Controls for the Authorised Business) of the DCC Licence;
 - (ii) the requirements of Sections G2 and G4 to G6 or any CPA Certificate Remedial Plan; and where:
 - (iii) following either a DCC Security Assessment, any material increase in the security risk relating to the DCC has been identified; or
 - (iv) the Security Sub-Committee otherwise considers it appropriate for that assessment to be carried out;
- (e) at the request of the Security Sub-Committee, provide to it advice in relation to:
 - (i) the compliance of the DCC with its obligations under SEC Section G or any CPA Certificate Remedial Plan; ~~and~~
 - ~~(ii)~~ changes in security risks relating to the Systems, Data, functionality and processes of the DCC which fall within SEC Section G5 (Information Security: Obligations on the DCC); ~~and~~
 - ~~(ii)(iii)~~ the compliance of the DCC with the obligations under SEC Appendix AC Section 5.20 and SEC Appendix AC Section 5.21;
- (f) at the request of the Security Sub-Committee, provide to it advice in relation to the suitability of any remedial action plan for the purposes of Section M8.4 of the Code (Consequences of an Event of Default);

- (g) at the request of the Security Sub-Committee Chair, provide a representative to attend and contribute to the discussion at any meeting of the Security Sub-Committee; and
 - (i) undertake such other activities and do so at such times and in such manner, as may be further provided for in this Section G9;
 - (ii) assess the DCC's compliance with the requirements of Condition 8 (Security Controls for the Authorised Business) of the DCC Licence;
 - (iii) such other requirements relating to the security of the DCC Total System as may be specified by the Security Sub-Committee or the Panel from time to time.

Appendix AC 'Inventory Enrolment and Decommissioning Procedures'

These changes have been redlined against Appendix AC version 7.0.

Add Section 5.20 to 5.23 as follows:

5. Post-Commissioning Obligations in relation to SMETS2+ Devices

General Obligations on DCC

- 5.18 The DCC shall monitor Responses it receives from Devices in order to determine whether any of the Device Certificates held on each Device have been successfully replaced. On the basis of this information the DCC shall establish and maintain a record of the most up-to-date active Device Certificates for each Device.
- 5.19 Where, following the addition of a Device to the Device Log of a Communications Hub Function, the DCC identifies that a Trust Anchor Cell of that Device 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, the DCC shall send a DCC Alert to the Responsible Supplier for the Device, notifying them of the situation.

Certificate Validity Periods

- 5.20 As soon as reasonably practicable (and in any event after 48 hours but before 7 days have elapsed) following the Commissioning of any Device that has one or more Trust Anchor Cells that are populated with information from an Organisation Certificate with a Remote Party Role of "transitionalCoS" that has a Validity Period of more than 10 years, the DCC shall take all reasonable steps to replace that information with that from an Organisation Certificate with a Remote Party Role of "transitionalCoS" that has a Validity Period of 10 years.
- 5.21 As soon as reasonably practicable (and in any event after seven days but before 23 days have elapsed) following the Commissioning of any Device that has one or more Trust Anchor Cells that are populated with information from an Organisation Certificate with a Remote Party Role of "accessControlBroker" that has a Validity Period of more than 10 years, the DCC shall take all reasonable steps to replace that information with that from an Organisation Certificate with a Remote Party Role of "accessControlBroker" that has a Validity Period of 10 years.

Revoked and Expired Certificates

- 5.22 As soon as reasonably practicable:
- (a) following the revocation of a Certificate from which information is used (in part) to populate the Device Security Credentials of any Device that forms part of an installed Smart Metering System; or
 - (b) following the installation of a Device (as part of a Smart Metering System) that holds Device Security Credentials that are populated (in part) with information from a Certificate that has been revoked, the Subscriber for the relevant Certificate shall take all reasonable steps to replace the relevant information with that from a Certificate that has not been revoked.
- 5.23 As soon as reasonably practicable:

- (a) before the expiry of the Validity Period of a Certificate from which information is used (in part) to populate the Device Security Credentials of any Device that forms part of an installed Smart Metering System; or
- (b) following the Commissioning of a Device (as part of a Smart Metering System) that holds Device Security Credentials that are populated (in part) with information from a Certificate that has a Validity Period that has expired, the Subscriber for that relevant Certificate shall take all reasonable steps to replace the relevant information with that from a Certificate that has a Validity Period that has not expired.