

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 0.1

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.

Add Section G.8.3 as follows:

G8. USER SECURITY ASSURANCE

Procurement of the User Independent Security Assurance Service Provider

G8.1 The Panel shall procure the provision of security assurance services:

- (a) of the scope specified in Section G8.3;
- (b) from a person who:
 - (i) is suitably qualified in accordance with Section G8.4;
 - (ii) is suitably independent in accordance with Section G8.7; and
 - (iii) satisfies the capacity requirement specified in Section G8.11,
- (c) and that person is referred to in this Section G8 as the “**User Independent Security Assurance Service Provider**”.

G8.2 The Panel may appoint more than one person to carry out the functions of the User Independent Security Assurance Service Provider.

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.

Suitably Qualified Service Provider

G8.4 The User Independent Security Assurance Service Provider shall be treated as suitably qualified in accordance with this Section G8.4 only if it satisfies:

- (a) the requirements specified in Section G8.5; and
- (b) the requirements specified in Section G8.6.

G8.5 The requirements specified in this Section G8.5 are that the User Independent Security Assurance Service Provider:

- (a) is accredited by UKAS as meeting the requirements for providing audit and certification of information security management systems in accordance with ISO/IEC 27001:2013 (Information Technology – Security Techniques – Information Security Management Systems) or any equivalent to that standard which updates or replaces it from time to time; and/or
- (b) holds another membership, accreditation, approval or form of professional validation that is in the opinion of the Security Sub-Committee substantially equivalent in status and effect to the arrangements described in paragraph (a).

G8.6 The requirement specified in this Section G8.6 is that the User Independent Security Assurance Service Provider:

- (a) employs consultants who are assured under an official cyber security qualification scheme recognised by NCSC or the UK Cyber Security Council or UKAS and which is approved by the Security Sub-Committee at levels equivalent to 'Chartered', 'Principal', 'Lead' or 'Senior Practitioner' in either the 'Security and Information Risk Advisor' or 'Information Assurance Auditor' roles; and
- (b) engages those individuals as its lead auditors for the purposes of carrying out all security assurance assessments in accordance with this Section G8.

Independence Requirement

G8.7 The User Independent Security Assurance Service Provider shall be treated as suitably independent in accordance with this Section G8.7 only if it satisfies:

- (a) the requirements specified in Section G8.9; and
- (b) the requirement specified in Section G8.10.

G8.8 For the purposes of Sections G8.9 and G8.10:

- (a) a "**Relevant Party**" means any Party in respect of which the User Independent Security Assurance Service Provider carries out functions under this Section G8; and
- (b) a "**Relevant Service Provider**" means any service provider to a Relevant Party from which that Party acquires capability for a purpose related to its compliance with its obligations as a User under Sections G3 to G6.

G8.9 The requirements specified in this Section G8.9 are that:

- (a) no Relevant Party or any of its subsidiaries, and no Relevant Service Provider or any of its subsidiaries, holds or acquires any investment by way of shares, securities or other financial rights or interests in the User Independent Security Assurance Service Provider;
- (b) no director of any Relevant Party, and no director of any Relevant Service Provider, is or becomes a director or employee of, or holds or acquires any investment by way of shares, securities or other financial rights or interests in, the User Independent Security Assurance Service Provider; and
- (c) the User Independent Security Assurance Service Provider does not hold or acquire a participating interest (as defined in section 421A of the Financial Services and Markets Act 2000) in any Relevant Party or any Relevant Service Provider,

(but for these purposes references to a Relevant Service Provider shall not include the User Independent Security Assurance Service Provider where it acts in that capacity).

G8.10 The requirement specified in this Section G8.10 is that the User Independent Security Assurance Service Provider is able to demonstrate to the satisfaction of the Panel that it has in place arrangements to ensure that it will at all times act independently of any commercial relationship that it has, has had, or may in future have with a Relevant Party or Relevant Service Provider (and for these purposes a 'commercial relationship' shall

include a relationship established by virtue of the User Independent Security Assurance Service Provider itself being a Relevant Service Provider to any Relevant Party).

Capacity Requirement

G8.11 The capacity requirement specified in this Section G8.11 is that the User Independent Security Assurance Service Provider must be capable of meeting the Panel's estimate of the demand for its security assurance services throughout the period in relation to which those services are being procured.

Compliance of the User Independent Security Assurance Service Provider

G8.12 The Panel shall be responsible for ensuring that the User Independent Security Assurance Service Provider carries out its functions in accordance with the provisions of this Section G8.

Users: Duty to Cooperate in Assessment

G8.13 Each User shall do all such things as may be reasonably requested by the Security Sub-Committee, or by any person acting on behalf of or at the request of the Security Sub-Committee (including in particular the User Independent Security Assurance Service Provider), for the purposes of facilitating an assessment of that User's compliance with its obligations under Sections G3 to G6 or any CPA Certificate Remedial Plan.

G8.14 For the purposes of Section G8.13, a User shall provide the Security Sub-Committee (or the relevant person acting on its behalf or at its request) with:

- (a) all such Data as may reasonably be requested, within such times and in such format as may reasonably be specified;
- (b) all such other forms of cooperation as may reasonably be requested, including in particular:
 - (i) access at all reasonable times to such parts of the premises of that User as are used for, and such persons engaged by that User as carry out or are authorised to carry out, any activities related to its compliance with its obligations under Sections G3 to G6; and
 - (ii) such cooperation as may reasonably be requested by the Independent Security Assessment Services Provider for the purposes of carrying out any security assurance assessment in accordance with this Section G8.

Categories of Security Assurance Assessment

G8.15 For the purposes of this Section G8, there shall be the following four categories of security assurance assessment:

- (a) a Full User Security Assessment (as further described in Section G8.16);
- (b) a Verification User Security Assessment (as further described in Section G8.17);
- (c) a User Security Self-Assessment (as further described in Section G8.18); and

(d) a Follow-up Security Assessment (as further described in Section G8.19).

G8.16 A **"Full User Security Assessment"** shall be an assessment carried out by the User Independent Security Assurance Service Provider in respect of a User to identify the extent to which that User is compliant with each of its obligations under Sections G3 to G6 in each of its User Roles.

G8.17 A **"Verification User Security Assessment"** shall be an assessment carried out by the User Independent Security Assurance Service Provider in respect of a User to identify any material increase in the security risk relating to the Systems, Data, functionality and processes of that User falling within Section G5.14 (Information Security: Obligations on Users) since the last occasion on which a Full User Security Assessment was carried out in respect of that User.

G8.18 A **"User Security Self-Assessment"** shall be an assessment carried out by a User, the outcome of which is reviewed by the User Independent Security Assurance Service Provider, to identify any material increase in the security risk relating to the Systems, Data, functionality and processes of that User falling within Section G5.14 (Information Security: Obligations on Users) since the last occasion on which a User Security Assessment was carried out in respect of that User.

G8.19 A **"Follow-up Security Assessment"** shall be an assessment carried out by the User Independent Security Assurance Service Provider, following a User Security Assessment, in accordance with the provisions of Section G8.29.

G8.20 For the purposes of Sections G8.17 and G8.18, a Verification Security Assessment and User Security Self-Assessment shall each be assessments carried out in respect of a User having regard in particular to:

- (a) any changes made to any System, Data, functionality or process falling within the scope of Section G5.14 (Information Security: Obligations on Users);
- (b) where the User is a Supplier Party, any increase in the number of Enrolled Smart Metering Systems for which it is the Responsible Supplier; and
- (c) where the User is a Network Party, any increase in the number of Enrolled Smart Metering Systems for which it is the Electricity Distributor or the Gas Transporter.

User Security Assessments: General Procedure

User Security Assessment Methodology

G8.21 Each User Security Assessment carried out by the User Independent Security Assurance Service Provider shall be carried out in accordance with the User Security Assessment Methodology applicable to the relevant category of assessment.

The User Security Assessment Report

G8.22 Following the completion of a User Security Assessment, the User Independent Security Assurance Service Provider shall, in discussion with the User to which the assessment relates, produce a written report (a **"User Security Assessment Report"**) which shall:

- (a) set out the findings of the User Independent Security Assurance Service Provider on all the matters within the scope of the User Security Assessment;
- (b) in the case of a Full User Security Assessment:
 - (i) specify any instances of actual or potential non-compliance of the User with its obligations under Sections G3 to G6 which have been identified by the User Independent Security Assurance Service Provider; and
 - (ii) set out the evidence which, in the opinion of the User Independent Security Assurance Service Provider, establishes each of the instances of actual or potential non-compliance which it has identified; and
- (c) in the case of a Verification User Security Assessment:
 - (i) specify any material increase in the security risk relating to that User which the User Independent Security Assurance Service Provider has identified since the last occasion on which a Full User Security Assessment was carried out in respect of that User; and
 - (ii) set out the evidence which, in the opinion of the User Independent Security Assurance Service Provider, establishes the increase in security risk which it has identified.

G8.23 The User Independent Security Assurance Service Provider shall submit a copy of each User Security Assessment Report to the Security Sub-Committee and to the User to which that report relates.

The User Security Assessment Response

G8.24 Following the receipt by any User of a User Security Assessment Report which relates to it, the User shall as soon as reasonably practicable, and in any event by no later than such date as the Security Sub-Committee may specify:

- (a) produce a written response to that report (a "**User Security Assessment Response**") which addresses the findings set out in the report; and
- (b) submit a copy of that response to the Security Sub-Committee and the User Independent Security Assurance Service Provider.

G8.25 Where a User Security Assessment Report:

- (a) following a Full User Security Assessment, specifies any instance of actual or potential non-compliance of a User with its obligations under Sections G3 to G6; or
- (b) following a Verification User Security Assessment, specifies any material increase in the security risk relating to a User since the last occasion on which a Full User Security Assessment was carried out in respect of that User,

the User shall ensure that its User Security Assessment Response includes the matters referred to in Section G8.26.

G8.26 The matters referred to in this Section are that the User Security Assessment Response:

- (a) indicates whether the User accepts the relevant findings of the User Independent Security Assurance Service Provider and, where it does not, explains why this is the case;
- (b) sets out any steps that the User has taken or proposes to take in order to remedy and/or mitigate the actual or potential non-compliance or the increase in security risk (as the case may be) specified in the User Security Assessment Report; and
- (c) identifies a timetable within which the User proposes to take any such steps that have not already been taken.

G8.27 Where a User Security Assessment Response sets out any steps that the User proposes to take in accordance with Section G8.26(b), the Security Sub-Committee (having considered the advice of the User Independent Security Assurance Service Provider) shall review that response and either:

- (a) notify the User that it accepts that the steps that the User proposes to take, and the timetable within which it proposes to take them, are appropriate to remedy and/or mitigate the actual or potential non-compliance or increase in security risk (as the case may be) specified in the User Security Assessment Report; or
- (b) seek to agree with the User such alternative steps and/or timetable as would, in the opinion of the Security Sub-Committee, be more appropriate for that purpose.

G8.28 Where a User Security Assessment Response sets out any steps that the User proposes to take in accordance with Section G8.26(b), and where those steps and the timetable within which it proposes to take them are accepted by the Security Sub-Committee, or alternative steps and/or an alternative timetable are agreed between it and the User in accordance with Section G8.27, the User shall:

- (a) take the steps that have been accepted or agreed (as the case may be) within the timetable that has been accepted or agreed (as the case may be); and
- (b) report to the Security Sub-Committee on:
 - (i) its progress in taking those steps, at any such intervals or by any such dates as the Security Sub-Committee may specify;
 - (ii) the completion of those steps in accordance with the timetable; and
 - (iii) any failure to complete any of those steps in accordance with the timetable, specifying the reasons for that failure.

Follow-up Security Assessment

G8.29 Where a User Security Assessment Response sets out any steps that the User proposes to take in accordance with Section G8.26(b), and where those steps and the timetable within which it proposes to take them are accepted by the Security Sub-Committee, or alternative steps and/or an alternative timetable are agreed between it and the User in accordance with Section G8.27, the User Independent Security

Assurance Service Provider shall, at the request of the Security Sub-Committee (and by such date as it may specify), carry out a Follow-up Security Assessment of the relevant User to:

- (a) identify the extent to which the User has taken the steps that have been accepted or agreed (as the case may be) within the timetable that has been accepted or agreed (as the case may be); and
- (b) assess any other matters related to the User Security Assessment Response that are specified by the Security Sub-Committee.

User Security Assessments: Further Provisions

G8.30 The User Independent Security Assurance Service Provider:

- (a) may in its discretion, and shall where directed to do so by the Security Sub-Committee:
 - (i) in relation to a User which acts in more than one User Role, determine that a single User Security Assessment may be carried out in relation to that User in respect of any two or more such User Roles; and
 - (ii) in carrying out any User Security Assessment, take into account any relevant security accreditation or certification held by the relevant User; and
- (b) shall, where any Shared Resources which have not been provided by a Shared Resource Provider form part of the User Systems of more than one User, have regard to information obtained in relation to such Shared Resources in the User Security Assessment of one such User when carrying out a User Security Assessment of any other such User.

Initial Full User Security Assessment: User Entry Process

G8.31 Sections G8.33 to G8.39 set out the applicable security requirements referred to in Section H1.10(c) (User Entry Process Requirements).

G8.32 For the purposes of Sections G8.33 to G8.39, any reference in Sections G3 to G6 or the preceding provisions of this Section G8 to a 'User' (or to any related expression which applies to Users), shall be read as including a reference (or otherwise applying) to any Party seeking to become a User by completing the User Entry Process for any User Role.

Initial Full User Security Assessment

G8.33 For the purpose of completing the User Entry Process for a User Role, a Party wishing to act as a User in that User Role shall be subject to a Full User Security Assessment in respect of the User Role.

Panel: Setting the Assurance Status

G8.34 Following the completion of that initial Full User Security Assessment, the Security Sub-Committee shall ensure that copies of both the User Security Assessment Report and User Security Assessment Response are provided to the Panel.

G8.35 Following the receipt by it of the User Security Assessment Report and User Security Assessment Response, the Panel shall promptly consider both documents and (having regard to any advice of the Security Sub-Committee) set the assurance status of the Party, in relation to its compliance with each of its obligations under Sections G3 to G6 in the relevant User Role, in accordance with Section G8.36.

G8.36 The Panel shall set the assurance status of the Party as one of the following:

- (a) approved;
- (b) approved, subject to the Party:
 - (i) taking such steps as it proposes to take in its User Security Assessment Response in accordance with Section G8.26(b); or
 - (ii) both taking such steps and being subject to a Follow-up Security Assessment by such date as the Panel may specify,
- (c) deferred and:
 - (i) the Party having first taken such steps as it proposes to take in its User Security Assessment Response in accordance with Section G8.26(b) and been subject to a Follow-up Security Assessment; and
 - (ii) the Panel having determined that it is satisfied, on the evidence of the Follow-up Security Assessment, that such steps have been taken; or
- (d) rejected and:
 - (i) the Party shall have a second Full User Security Assessment to address any issues identified by the Panel as being, in the opinion of the Panel, not adequately addressed in that response as submitted to the Security Sub-Committee; and
 - (ii) upon completion of the second Full User Security Assessment the Panel will reconsider the assurance status in accordance with Section G8.35.

Approval

G8.37 For the purposes of Sections H1.10(c) and H1.11 (User Entry Process Requirements):

- (a) a Party shall be considered to have successfully demonstrated that it meets the applicable security requirements of this Section G8 when:
 - (i) the Panel has set its assurance status to 'approved' in accordance with either Section G8.36(a) or (b); or

- (ii) the Panel has set its assurance status to 'deferred' in accordance with Section G8.36(c) and the requirements specified in that Section have been met; and
- (b) the Panel shall notify the Code Administrator as soon as reasonably practicable after the completion of either event described in paragraph (a)(i) or (ii).

Obligations on an Approved Party

G8.38 Where the Panel has set the assurance status of a Party to 'approved subject to' specified in Section G8.36(b), the Party shall take the steps to which that approval is subject in accordance with that section.

Disagreement with Panel Decisions

G8.39 Where a Party disagrees with any decision made by the Panel in relation to it under Section G8.36, it may appeal that decision to the Authority and the determination of the Authority shall be final and binding for the purposes of the Code.

Security Assurance Assessments: Post-User Entry Process

G8.40 Within 12 months after completion of the User's initial Full User Security Assessment (or after the Follow-up Security Assessment where there was one), for the purposes of the User Entry Process, a User shall schedule a User Security Assessment with the User Independent Security Assurance Provider in accordance with the provisions of Sections G8.41 to G8.47. The initial Full User Security Assessment will be deemed complete when the Panel set an assurance status of:

- (a) approved; or
- (b) approved, subject to the User:
 - (i) taking such steps as the User proposes to take in its User Security Assessment Response in accordance with Section G8.26(b); or
 - (ii) both taking the steps referred to in (i) above and being subject to a Follow-up Security Assessment by such date as the Panel may specify.

Supplier Parties

G8.41 Where a User is a Supplier Party and either:

- (a) the number of Domestic Premises supplied with electricity and/or gas through one or more Smart Metering Systems for which it is the Responsible Supplier exceeds 250,000; or
- (b) the number of Non-Domestic Premises supplied with electricity and/or gas through one or more Smart Metering Systems for which it is the Responsible Supplier exceeds 50,000; or
- (c) $(5N) + D > 250,000$

Where N is the number of Non-Domestic Premises and D is the number of Domestic Premises supplied with electricity and/or gas through one or more Smart Metering Systems for which it is the Responsible Supplier,

the User Security Assessment required by Section G8.40 shall be a Full User Security Assessment and the User shall schedule a further Full User Security Assessment within 12 months after each Full User Security Assessment.

G8.42 Where a User is a Supplier Party of electricity and/or gas to Domestic Premises and/or Non-Domestic Premises through one or more Smart Metering Systems for which it is the Responsible Supplier but does not meet any of the criteria specified under Section G8.41, the User Security Assessment required by Section G8.40 shall be a Verification User Security Assessment and the User shall:

- (a) within 12 months after each Verification User Security Assessment schedule a User Security Self-Assessment; and
- (b) within 12 months after each User Security Self-Assessment, schedule a Full User Security Assessment with the User Independent Security Assurance Service Provider; and
- (c) within 12 months after each Full User Security Assessment, schedule a Verification User Security Assessment with the User Independent Security Assurance Service Provider.

G8.43 In assessing for the purposes of Sections G8.41 and G8.42 the number of Domestic Premises and Non-Domestic Premises supplied with electricity and/or gas through one or more Smart Metering Systems for which a User is the Responsible Supplier, that number shall, where any Shared Resources which are not provided by a Shared Resource Provider form part of both its User Systems and the User Systems of another User, be deemed to include any Domestic Premises or Non-Domestic Premises supplied with electricity and/or gas through one or more Smart Metering Systems for which that other User is the Responsible Supplier.

Network Parties

G8.44 Where a User is a Network Party and the number of Domestic Premises supplied with electricity and/or gas through one or more Smart Metering Systems for which it is the Electricity Distributor and/or the Gas Transporter exceeds 250,000, the User Security Assessment required by Section G8.40 shall be a Verification User Security Assessment and the User shall:

- (a) within 12 months after previous Verification User Security Assessment, schedule a second Verification User Security Assessment with the User Independent Security Assurance Provider;
- (b) within 12 months after each second successive Verification User Security Assessment, schedule a Full User Security Assessment with the User Independent Security Assurance Service Provider; and

- (c) within 12 months after each Full User Security Assessment, schedule a Verification User Security Assessment with the User Independent Security Assurance Service Provider.

G8.45 Where a User is a Network Party and the number of Domestic Premises supplied with electricity and/or gas through one or more Smart Metering Systems for which it is the Electricity Distributor and/or the Gas Transporter is equal to or less than 250,000, the User Security Assessment required by Section G8.40 shall be a Verification User Security Assessment and the User shall:

- (a) within 12 months after each Verification User Security Assessment, schedule a User Security Self-Assessment;
- (b) within 12 months after each User Security Self-Assessment, schedule a Full User Security Assessment with the User Independent Security Assurance Service Provider; and
- (c) within 12 months after each Full User Security Assessment, schedule a Verification User Security Assessment with the User Independent Security Assurance Service Provider.

G8.46 In assessing for the purposes of Sections G8.44 and G8.45 the number of Domestic Premises supplied with electricity and/or gas through one or more Smart Metering Systems for which a User is the Electricity Distributor and/or the Gas Transporter, that number shall, where any Shared Resources form part of both its User Systems and the User Systems of another User, be deemed to include any Domestic Premises supplied with electricity and/or gas through one or more Smart Metering Systems for which that other User is the Electricity Distributor and/or the Gas Transporter.

Other Users

G8.47 Where a User is neither a Supplier Party nor a Network Party, Section G8.40 requires the User to schedule a User Security Verification Assessment and the User shall:

- (a) within 12 months after the previous User Security Verification Assessment, schedule a User Security Self-Assessment;
- (b) within 12 months after the User Security Self-Assessment schedule a Full User Security Assessment with the User Independent Security Assurance Service Provider; and
- (c) within 12 months after each Full User Security Assessment, schedule a User Security Verification Assessment.

Interpretation

G8.48 Section G8.49 applies where:

- (a) pursuant to Sections G8.41 to G8.43, it is necessary to determine, in relation to any Supplier Party, the number of Domestic Premises and Non-Domestic Premises that are supplied with electricity and/or gas through one or more Smart Metering Systems for which it is the Responsible Supplier; or

Managed by

- (b) pursuant to Sections G8.44 to G8.46, it is necessary to determine, in relation to any Network Party, the number of Domestic Premises that are supplied with electricity and/or gas through one or more Smart Metering Systems for which it is the Electricity Distributor and/or the Gas Transporter.

G8.49 Where this Section applies:

- (a) the determination referred to in Section G8.48 shall be made at the time at which the nature of each annual security assurance assessment for the relevant User falls to be ascertained; and
- (b) the DCC shall provide all reasonable assistance that may be requested by that User or the Security Sub-Committee for the purposes of making that determination.

User Security Self-Assessment

G8.50 Where, in accordance with the requirements of this Section G8, a User is subject to a User Security Self-Assessment in any year, that User shall:

- (a) carry out the User Security Self-Assessment during in accordance with the User Security Assessment Methodology that is applicable to User Security Self-Assessments; and
- (b) ensure that the outcome of the User Security Self-Assessment is documented and is submitted to the User Independent Security Assurance Service Provider for review by no later than the date which is 12 months after the date of the completion of the previous User Security Assessment or (if more recent) User Security Self-Assessment.

Users: Obligation to Pay Explicit Charges

G8.51 Each User shall pay to the DCC all applicable Charges in respect of:

- (a) all User Security Assessments and Follow-up Security Assessments carried out in relation to it by the User Independent Security Assurance Service Provider;
- (b) the production by the User Independent Security Assurance Service Provider of any User Security Assessment Reports following such assessments; and
- (c) all related activities of the User Independent Security Assurance Service Provider in respect of that User in accordance with this Section G8.

G8.52 Expenditure incurred in relation to Users in respect of the matters described in Section G8.51 shall be treated as Recoverable Costs in accordance with Section C8 (Panel Costs and Budgets).

G8.53 For the purposes of Section G8.51 the Panel shall, at such times and in respect of such periods as it may (following consultation with the DCC) consider appropriate, notify the DCC of:

- (a) the expenditure incurred in respect of the matters described in Section G8.51 that is attributable to individual Users, in order to facilitate Explicit Charges designed to

pass-through the expenditure to such Users pursuant to Section K7 (Determining Explicit Charges); and

- (b) any expenditure incurred in respect of the matters described in Section G8.51 which cannot reasonably be attributed to an individual User.

Events of Default

G8.54 In relation to an Event of Default which consists of a material breach by a User of any of its obligations under Sections G3 to G6, the provisions of Sections M8.2 to M8.4 shall apply subject to the provisions of Sections G8.55 to G8.60.

G8.55 Where in accordance with Section M8.2 the Panel receives notification that a User is in material breach of any requirements of Sections G3 to G6, it shall refer the matter to the Security Sub-Committee.

G8.56 On any such referral the Security Sub-Committee may investigate the matter in accordance with Section M8.3 as if the references in that Section to the “Panel” were to the “Security Sub-Committee”.

G8.57 Where the Security Sub-Committee has:

- (a) carried out an investigation in accordance with Section M8.3; or
- (b) received a report from the User Independent Security Assurance Service Provider, following a User Security Assessment, concluding that a User is in actual or potential non-compliance with any of its obligations under Sections G3 to G6,

the Security Sub-Committee shall consider the information available to it and, where it considers that actual non-compliance with any obligations under Sections G3 to G6 has occurred, shall refer the matter to the Panel for it to determine whether that non-compliance constitutes an Event of Default.

G8.58 Where the Panel determines that an Event of Default has occurred, it shall:

- (a) notify the relevant User and any other Party it considers may have been affected by the Event of Default; and
- (b) determine the appropriate steps to take in accordance with Section M8.4.

G8.59 Where the Panel is considering what steps to take in accordance with Section M8.4, it may request and consider the advice of the Security Sub-Committee.

G8.60 Where the Panel determines that a User is required to give effect to a remedial action plan in accordance with Section M8.4(d) that plan must be approved by the Panel (having regard to any advice of the Security Sub-Committee).

Shared Resource Providers

G8.61 Section G8.62 applies where:

- (a) Shared Resources are provided to a User by a Shared Resource Provider; and

- (b) any User Security Assessment is carried out in respect of that Shared Resource Provider.

G8.62 Where this Section applies:

- (a) the outcome of the User Security Assessment (including for these purposes any actions or decisions described at Sections G8.22 to G8.29) shall be treated as applying to the User, in respect of the Shared Resources, in the same manner as it is applicable to the Shared Resource Provider; and
- (b) in any User Security Assessment which takes place in respect of the User, the User Independent Security Assessment Service Provider shall, with regard to matters relating to the Shared Resources, rely on the outcome of the most recent User Security Assessment in respect of the Shared Resource Provider and shall not be required to repeat that assessment.

G8.63 For the purposes of Section G8.40, where a Shared Resource Provider provides Shared Resources to Users which are:

- (a) Supplier Parties, the provisions of Sections G8.41 and G8.42 shall apply to the Shared Resource Provider as if it was a Supplier Party and the Smart Metering Systems for which those Supplier Parties are the Responsible Suppliers were Smart Metering Systems for which it is the Responsible Supplier;
- (b) Network Parties, the provisions of Sections G8.44 to G8.46 shall apply to the Shared Resource Provider as if it was a Network Party and the Smart Metering Systems for which those Network Parties are the Electricity Distributor and/or Gas Transporter were Smart Metering Systems for which it is the Electricity Distributor and/or Gas Transporter;
- (c) Other Users, the provisions of Section G8.47 shall apply to the Shared Resource Provider as if it was an Other User.

CPA Certificate Remedial Plan Preparation

G8.64 Where a User is a Supplier Party, the User shall ensure that it has in place (and periodically reviews) a policy for creating and managing compliance with CPA Certificate Remedial Plans.

Add Section G9.2 as follows:

G9. DCC SECURITY ASSURANCE

The DCC Independent Security Assessment Arrangements

G9.1 The DCC shall establish, give effect to, maintain and comply with arrangements, to be known as the "**DCC Independent Security Assessment Arrangements**", which shall procure the services of a DCC Independent Security Assessment Service Provider to undertake security assessment services.

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 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.

G9.3 The actions specified in this Section G9.3 shall be actions taken by the DCC to:

- (a) procure the provision of security assessment services by the DCC Independent Security Assessment Service Provider (as further described in Section G9.4);
- (b) ensure that the DCC Independent Security Assessment Service Provider carries out Security Assessments for the purpose specified in Section G9.2:
 - (i) annually;
 - (ii) on any material change to the DCC Total System; and
 - (iii) at any other time specified by the Security Sub-Committee or the Panel;
- (c) comply with the arrangements set out by the Security Sub-Committee in a Security Controls Framework;
- (d) in line with the methodology and processes set out in the Security Controls Framework:
 - (i) procure that the DCC Independent Security Assessment Service Provider produces a DCC Security Assessment Report following each such assessment that has been carried out;
 - (ii) ensure that the DCC Independent Security Assessment Service Provider provides the Security Sub-Committee with a copy of each such DCC Security Assessment Report;
 - (iii) produce a DCC Security Assessment Response in relation to each such report; and
 - (iv) provide to the Panel and the Security Sub-Committee a copy of each DCC Security Assessment Response and, as soon as reasonably practicable thereafter, a report on its implementation of any action plan that is required by the Security Sub-Committee.

The DCC Independent Security Assessment Service Provider

G9.4 For the purposes of Section G9.3, the "**DCC Independent Security Assessment Service Provider**" shall be a person who is appointed by the DCC to provide security assessment services:

- (a) of the scope specified in Section G9.2;
- (b) from a person who:

- (i) is suitably qualified in accordance with Section G9.5;
- (ii) is suitably independent in accordance with Section G9.8.

Suitably Qualified Service Provider

G9.5 The DCC Independent Security Assessment Service Provider shall be treated as suitably qualified in accordance with this Section G9.5 only if it satisfies:

- (a) the requirements specified in Section G9.6; and
- (b) the requirement specified in Section G9.7.

G9.6 The requirements specified in this Section G9.6 are that the DCC Independent Security Assessment Service Provider:

- (a) is accredited by UKAS as meeting the requirements for providing audit and certification of information security management systems in accordance with ISO/IEC 27001:2017 Information Technology – Security Techniques – Information Security Management Systems) or any equivalent to that standard which updates or replaces it from time to time; and/or
- (b) holds another membership, accreditation, approval or form of professional validation that is in the opinion of the Security Sub-Committee substantially equivalent in status and effect to the arrangements described in paragraph (a).

G9.7 The requirement specified in this Section G9.7 is that the DCC Independent Security Assessment Service Provider:

- (a) employs consultants who are assured under an official cyber security qualification scheme recognised by NCSC or the UK Cyber Security Council or UKAS and which is approved by the Security Sub-Committee at levels equivalent to 'Chartered', 'Principal', 'Lead' or 'Senior Practitioner' in either 'Security and Information Risk Advisor' or 'Information Assurance Auditor' roles; and
- (b) engages those individuals as its lead auditors for the purposes of carrying out all security assessments in accordance with this Section G7.

Independence Requirement

G9.8 The DCC Independent Security Assurance Service Provider shall be treated as suitably independent in accordance with this Section G9.8 only if it satisfies:

- (a) the requirements specified in Section G9.9; and
- (b) the requirement specified in Section G9.10.

G9.9 For the purposes of Sections G9.9 and G9.10:

- (a) the DCC must be independent from the DCC Independent Security Assessment Service Provider in carrying out functions under this Section G9; and

- (b) all of the DCC's Service Providers must be independent from the DCC Independent Security Assessment Service Provider in carrying out its functions to assess the DCC's compliance with its obligations as the DCC under Sections G2 and G4 to G6 and DCC Licence Condition 8 (Security Controls for the Authorised Business) and SEC Appendix Z Sections 6 and 7.

G9.10 The requirements specified in this Section G9.10 are that:

- (a) neither the DCC or any of its subsidiaries, and no DCC Service Provider or any of its subsidiaries, holds or acquires any investment by way of shares, securities or other financial rights or interests in the DCC Independent Security Assessment Service Provider;
- (b) no director of the DCC and no director of any DCC Service Provider, is or becomes a director or employee of, or holds or acquires any investment by way of shares, securities or other financial rights or interests in, the DCC Independent Security Assessment Service Provider; and
- (c) the DCC Independent Security Assessment Service Provider does not hold or acquire a participating interest (as defined in section 421A of the Financial Services and Markets Act 2000) in the DCC or any of the DCC's Service Providers, (for these purposes references to the DCC's Service Providers shall not include the DCC Independent Security Assessment Service Provider where it acts in that capacity).

G9.11 The requirement specified in this Section G9.11 is that the DCC Independent Security Assessment Service Provider is able to demonstrate to the satisfaction of the Security Sub-Committee that it has in place arrangements to ensure that it will at all times act independently of any commercial relationship that it has, has had, or may in future have with the DCC or the DCC's Service Providers (and for these purpose a 'commercial relationship' shall include a relationship established by virtue of the DCC Independent Security Assessment Service Provider itself being a DCC Service Provider to the DCC).

Compliance of the DCC Independent Security Assessment Service Provider

G9.12 The Security Sub-Committee shall advise the DCC of any performance failures or non-compliance with the SEC obligations on the part of the DCC Independent Security Assessment Service Provider to enable the DCC to ensure that the DCC Independent Security Assessment Service Provider carries out its functions in accordance with the provisions of this Section G12.

DCC: Duty to Cooperate in Assessment

G9.13 The DCC shall do all such things as may be reasonably requested by the Security Sub-Committee, or by any person acting on behalf of or at the request of the Security Sub-Committee (including in particular the DCC Independent Security Assessment Service Provider), for the purposes of facilitating an assessment of the DCC's compliance with its obligations under Sections G2 and G4 to G6 or DCC Licence Condition 8 (Security Controls for the Authorised Business) or SEC Appendix Z Sections 6 and 7 and any CPA Certificate Remedial Plan.

G9.14 For the purposes of Section G9.13, the DCC shall provide the DCC Independent Security Assessment Service Provider with:

- (a) all such Data as may reasonably be requested, within such times and in such format as may reasonably be specified;
- (b) all such other forms of cooperation as may reasonably be requested, including in particular:
 - (i) access at all reasonable times to such parts of the premises of the DCC or its Service Providers as are used for, and such persons engaged by the DCC as carry out or are authorised to carry out, any activities related to its compliance with its obligations under Sections G2 and G4 to G6 and DCC Licence Condition 8 (Security Controls for the Authorised Business) and SEC Appendix Z Sections 6 and 7; and
 - (ii) such cooperation as may reasonably be requested by the DCC Independent Security Assessment Services Provider for the purposes of carrying out any security assurance assessment in accordance with this Section G9.

Categories of DCC Security Assessment

G9.15 For the purposes of this Section G9, there shall be the following two categories of security assessment:

- (a) a Full DCC Security Assessment (as further described in Section G9.16);
- (b) a Follow-up DCC Security Assessment (as further described in Section G9.17).

G9.16 A **"Full DCC Security Assessment"** shall be an assessment carried out by the DCC Independent Security Assessment Service Provider in respect of the DCC and its Service Providers to identify the extent to which the DCC is compliant with each of its obligations under Sections G2 and G4 to G6 and DCC Licence Condition 8 (Security Controls for the Authorised Business) and SEC Appendix Z Sections 6 and 7.

G9.17 A **"Follow-up DCC Security Assessment"** shall be an assessment carried out by the DCC Independent Security Assessment Service Provider, following a DCC Security Assessment, in accordance with the provisions of Section G9.25.

DCC Security Assessments: General Procedure

DCC Security Assessment Methodology

G9.18 Each DCC Security Assessment carried out by the DCC Independent Security Assessment Service Provider shall be carried out in accordance with the Security Controls Framework developed as defined in G7.19(a).

The DCC Security Assessment Report

G9.19 Following the completion of a DCC Security Assessment, the DCC Independent Security Assessment Service Provider shall, in discussion with the DCC, produce a written report (a **"DCC Security Assessment Report"**) which shall:

- (a) set out the findings of the DCC Independent Security Assessment Service Provider on all the matters within the scope of the DCC Security Assessment;
- (b) specify any instances of actual or potential non-compliance of the DCC with its obligations under Sections G2 and G4 to G6 which have been identified by the DCC Independent Security Assessment Service Provider;
- (c) specify any instances of actual or potential non-compliance of the DCC with its obligations under DCC Licence Condition 8 (Security Controls for the Authorised Business);
- (d) specify any instances of actual or potential non-compliance of the DCC with its obligations under SEC Appendix Z, Sections 6 and 7; and
- (e) set out the evidence which, in the opinion of the DCC Independent Security Assessment Service Provider, establishes each of the instances of actual or potential non-compliance which it has identified.

G9.20 The DCC Independent Security Assessment Service Provider shall submit a copy of each DCC Security Assessment Report to the Security Sub-Committee and to the DCC.

The DCC Security Assessment Response

G9.21 Following the receipt by the DCC of a DCC Security Assessment Report which relates to it, the DCC shall as soon as reasonably practicable, and in any event by no later than such date as the Security Sub-Committee may specify:

- (a) produce a written response to that report (a "**DCC Security Assessment Response**") which addresses the findings set out in the report; and
- (b) submit a copy of that response to the Security Sub-Committee and the DCC Independent Security Assessment Service Provider.

G9.22 Where a DCC Security Assessment Report following a Full DCC Security Assessment, specifies any instance of actual or potential non-compliance of the DCC with its obligations under Sections G2 and G4 to G6 and/or with DCC Licence Condition 8 (Security Controls for the Authorised Business) and/or with SEC Appendix Z, Sections 6 and 7, the DCC shall ensure that its DCC Security Assessment response includes the matters referred to in Section G9.23.

G9.23 The matters referred to in this Section are that the DCC Security Assessment Response:

- (a) indicates whether the DCC accepts the relevant findings of the DCC Independent Security Assessment Service Provider and, where it does not, explains why this is the case;
- (b) sets out any steps that the DCC has taken or proposes to take in order to remedy and/or mitigate the actual or potential non-compliance or the increase in security risk (as the case may be) specified in the DCC Security Assessment Report; and

- (c) identifies a timetable within which the DCC proposes to take any such steps that have not already been taken.

G9.24 Where a DCC Security Assessment Response sets out any steps that the DCC proposes to take in accordance with Section G9.23(b), the Security Sub-Committee (having considered the advice of the DCC Independent Security Assessment Service Provider) shall review that response and either:

- (a) notify the DCC that it accepts that the steps that the DCC proposes to take, and the timetable within which it proposes to take them, are appropriate to remedy and/or mitigate the actual or potential non-compliance or increase in security risk (as the case may be) specified in the DCC Security Assessment Report; or
- (b) seek to agree with the DCC such alternative steps and/or timetable as would, in the opinion of the Security Sub-Committee, be more appropriate for that purpose.

G9.25 Where a DCC Security Assessment Response sets out any steps that the DCC proposes to take in accordance with Section G9.23(b), and where those steps and the timetable within which it proposes to take them are accepted by the Security Sub-Committee, or alternative steps and/or an alternative timetable are agreed between it and the DCC in accordance with Section G9.24(b), the DCC shall:

- (a) take the steps that have been accepted or agreed (as the case may be) within the timetable that has been accepted or agreed (as the case may be); and
- (b) report to the Security Sub-Committee on:
 - (i) its progress in taking those steps, at any such intervals or by any such dates as the Security Sub-Committee may specify;
 - (ii) the completion of those steps in accordance with the timetable; and
 - (iii) any failure to complete any of those steps in accordance with the timetable, specifying the reasons for that failure.

Follow-up Security Assessment

G9.26 Where a DCC Security Assessment Response sets out any steps that the User proposes to take in accordance with Section G9.23(b), and where those steps and the timetable within which it proposes to take them are accepted by the Security Sub-Committee, or alternative steps and/or an alternative timetable are agreed between it and the User in accordance with Section G9.24(b), the DCC Independent Security Assessment Service Provider shall, at the request of the Security Sub-Committee (and by such date as it may specify), carry out a Follow-up Security Assessment of the DCC to:

- (a) identify the extent to which the DCC has taken the steps that have been accepted or agreed (as the case may be) within the timetable that has been accepted or agreed (as the case may be); and
- (b) assess any other matters related to the DCC Security Assessment Response that are specified by the Security Sub-Committee.

DCC Security Assessments: Further Provisions

G9.27 The DCC Independent Security Assessment Service Provider may, in carrying out any DCC Security Assessment, take into account any relevant security accreditation or certification held by the DCC.

Setting the Compliance Status

G9.28 Following the completion of a Full DCC Security Assessment, the Security Sub-Committee shall consider the DCC Security Assessment Report and the DCC Security Assessment Response.

G9.29 The Security Sub-Committee shall identify whether any remaining non-compliances that exist with Section G2 or G4 to G6 and/or the DCC Licence Condition 8 (Security Controls for the Authorised Business) and/or SEC Appendix Z, Sections 6 and 7 and shall, where appropriate:

- (a) note and record that there are no non-compliances; or
- (b) note and record the specific non-compliances that need to be addressed.

G9.30 Where the Security Sub-Committee identifies remaining non-compliances that exist with Section G2 and G4 to G6 and/or the DCC Licence Condition 8 (Security Controls for the Authorised Business) and/or SEC Appendix Z Sections 6 and 7, it shall:

- (a) require the DCC to take the steps set out in Section G9.24: or
- (b) require a Follow-up Security Assessment as set out in Section G9.26.

G9.31 Where the Security Sub-Committee identifies any remaining non-compliances with Section G2 or G4 to G6 and/or the DCC Licence Condition 8 (Security Controls for the Authorised Business) and/or SEC Appendix Z, Sections 6 and 7, it shall notify the Panel as required by G9.37(b).

CPA Certificate Remedial Plan Preparation

G9.32 The DCC shall ensure that it has in place (and periodically reviews) a policy for creating and managing compliance with CPA Certificate Remedial Plans. The DCC Independent Security Assessment Service Provider will assess the DCC's compliance with Appendix Z Section 6 and Section 7.

Disagreement with Security Sub-Committee Decisions

G9.33 Where the DCC disagrees with any decision made by the Security Sub-Committee in relation to it under Section G9.28 to G9.31, it may appeal that decision to the Panel. If the DCC disagrees with any decision made by the Panel, it may appeal that decision to the Authority and the determination of the Authority shall be final and binding for the purposes of the Code.

Events of Default

G9.34 In relation to an Event of Default which consists of a material breach by the DCC of any of the obligations referred to at Section G9.2(c), the provisions of Sections M8.2 to M8.4 shall apply subject to the provisions of Sections G9.35 to G9.41.

G9.35 For the purposes of Sections M8.2 to M8.4 as they apply pursuant to Section G9.34, an Event of Default shall (notwithstanding the ordinary definition thereof) be deemed to have occurred in respect of the DCC where it is in material breach of any of the obligations referred to at Section G9.2(d) (provided that Sections M8.4(e), (f) and (g) shall never apply to the DCC).

G9.36 Where in accordance with Section M8.2 the Panel receives notification that the DCC is in material breach of any of the obligations referred to at Section G9.2(d), it shall refer the matter to the Security Sub-Committee.

G9.37 On any such referral the Security Sub-Committee may investigate the matter in accordance with Section M8.3 as if the references in that Section to the “Panel” were to the “Security Sub-Committee”.

G9.38 Where the Security Sub-Committee has:

- (a) carried out an investigation in accordance with Section M8.3; or
- (b) received a DCC Security Assessment Report concluding that the DCC is in actual or potential non-compliance with any of the obligations referred to at Section G9.2(c),

the Security Sub-Committee shall consider the information available to it and, where it considers that actual non-compliance with any of the obligations referred to at Section G9.2(c) has occurred, shall refer the matter to the Panel for it to determine whether that non-compliance constitutes an Event of Default.

G9.39 Where the Panel determines that an Event of Default has occurred, it shall:

- (a) notify the DCC and any other Party it considers may have been affected by the Event of Default; and
- (b) determine the appropriate steps to take in accordance with Section M8.4.

G9.40 Where the Panel is considering what steps to take in accordance with Section M8.4, it may request and consider the advice of the Security Sub-Committee.

G9.41 Where the Panel determines that the DCC is required to give effect to a remedial action plan in accordance with Section M8.4(d) that plan must be approved by the Panel (having regard to any advice of the Security Sub-Committee).

CPA Certificate Remedial Plan Preparation

G9.42 The DCC shall ensure that it has in place (and periodically reviews) a policy for creating and managing compliance with CPA Certificate Remedial Plans.

Appendix AC 'Inventory Enrolment and Decommissioning Procedures'

These changes have been redlined against Appendix AC version 7.0.

Add Section 5.19 as follows:

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

- 5.1 This Clause 5 applies only to SMETS2+ Devices.
- 5.2 As soon as reasonably practicable (and in any event within 7 days) following the Commissioning of a Communications Hub Function, the DCC shall ensure that:
 - (a) the Communications Hub Function re-generates its Private Keys, and that Device Certificates containing the associated new Public Keys are stored on the Device; and
 - (b) the information from at least one of the Organisation Certificates that comprise the Communications Hub Function's Device Security Credentials is replaced (provided that for such purposes the information from an Organisation Certificate may be replaced with that from the same Organisation Certificate).
- 5.3 As soon as reasonably practicable (and in any event within 7 days) following the Commissioning of a Smart Meter, a Standalone Auxiliary Proportional Controller or a Gas Proxy Function, the Responsible Supplier shall, in relation to each such Device, ensure that:
 - (a) the Device Security Credentials which pertain to the Network Parties are:
 - (i) in the case of those which pertain to the Electricity Network Party, those of the Electricity Distributor; and
 - (ii) in the case of those which pertain to the Gas Network Party, those of the Gas Transporter (or, if they are not available in the SMKI Repository, the Device Security Credentials which pertain to the Gas Network Party shall be populated with information from the Organisation Certificates Issued to the DCC and referred to in Sections L3.23(f) (the DCC (access-Control-Broker) – digitalSignature Certificate) and L3.23(g) (the DCC (access-Control-Broker) – keyAgreement Certificate));
 - (b) the Device re-generates its Private Keys, and that the Device Certificates containing the associated new Public Keys are stored on the Device; and
 - (c) in the case of a Smart Meter and a Standalone Auxiliary Proportional Controller, information from at least one of the Organisation Certificates that comprise the Device's Device Security Credentials is replaced (provided that for such purposes the information from an Organisation Certificate may be replaced with that from the same Organisation Certificate).
- 5.4 As soon as reasonably practicable (and in any event within 7 days) following the Commissioning of a Communications Hub Function, Gas Proxy Function, Standalone

Managed by

Auxiliary Proportional Controller or Smart Meter, the DCC shall interrogate the Device to ascertain whether the Device's recovery Trust Anchor Cell is populated with Device Security Credentials that pertain to a DCC Recovery Certificate. For Devices Commissioned before Service Release 1.3 (or such later date as may be directed by the SofS for the purposes of this Clause 5.4), the reference to the period of 7 days following Commissioning shall apply as 7 days following Service Release 1.3 (or 7 days following any later date directed by the SofS).

- 5.5 The DCC shall monitor Commands sent to Devices and the associated Responses from Devices and, based on the information available to it, record the information set out in Clause 5.8 in relation to each Device identified in Clause 5.7 (the **"Post Commissioning Information"**).
- 5.6 The DCC shall ensure that the Post Commissioning Information is updated on a daily basis to reflect the most accurate and up-to-date information available to the DCC at the time of the update.
- 5.7 For the purposes of Clause 5.5, the relevant Devices include any Communications Hub Function, Gas Proxy Function, a Standalone Auxiliary Proportional Controller or Smart Meter which has an SMI Status of 'commissioned', has been Commissioned for a period of 7 days or more, and in relation to which one or both of the following applies:
 - (a) the DCC has failed successfully to carry out the interrogation of the Device pursuant to Clause 5.4; and/or
 - (b) the DCC has successfully carried out the interrogation of the Device pursuant to Clause 5.4 and has identified that the Device's recovery Trust Anchor Cell is not populated with Device Security Credentials that pertain to a DCC Recovery Certificate.
- 5.8 For the purposes of Clause 5.5, the Post Commissioning Information to be recorded in relation to each relevant Device shall include:
 - (a) the Device ID and Device Type;
 - (b) the date upon which the Device was Commissioned;
 - (c) which of Clauses 5.7 (a) and/or (b) applies;
 - (d) other than in the case of Communications Hub Functions, the Responsible Supplier at the time the Post Commissioning Information for the Device was most recently updated;
 - (e) other than in the case of Communications Hub Functions, the Supplier Party that sent the Service Request that resulted in the Commissioning of the Device; and
 - (f) the date on which the Post Commissioning Information for the Device was most recently updated.
- 5.9 As soon as reasonably practicable following the end of each month, the DCC shall, based upon the Post Commissioning Information prevailing at the end of that month, compile and provide (in an electronic format) to the Panel, the Security Sub-Committee and the Authority a report which includes the following information:

- (a) the month to which the report relates;
- (b) for each Party that is the Responsible Supplier for any Smart Meter or Gas Proxy Function that is listed in the Post Commissioning Information for that month (or was listed in the information for the previous month):
 - (i) the total number of Devices of each Device Type listed in the Post Commissioning Information for that month for which that Party is the Responsible Supplier;
 - (ii) the number of such Devices of each Device Type that have been added since the last monthly report;
 - (iii) the number of such Devices of each Device Type that have been removed since the last monthly report;
 - (iv) the number of such Devices of each Device Type that were listed in the Post Commissioning Information for the previous month and remain listed in the information for the month to which the report relates;
 - (v) the number of such Devices of each Device Type that were listed in the Post Commissioning Information for the previous three months and remain listed in the information for the month to which the report relates; and
 - (vi) the number of such Devices of each Device Type that were listed in the Post Commissioning Information for the previous six months and remain listed in the information for the month to which the report relates; and
- (c) in respect of Communications Hub Functions:
 - (i) the total number of Communications Hub Functions listed in the Post Commissioning Information;
 - (ii) the number of Communications Hub Functions that have been added since the last monthly report;
 - (iii) the number of Communications Hub Functions that have been removed since the last monthly report;
 - (iv) the number of Communications Hub Functions that were listed in the Post Commissioning Information for the previous month and remain listed in the information for the month to which the report relates;
 - (v) the number of Communications Hub Functions that were listed in the Post Commissioning Information for the previous three months and remain listed in the information for the month to which the report relates; and
 - (vi) the number of Communications Hub Functions that were listed in the Post Commissioning Information for the previous six months and remain listed in the information for the month to which the report relates.

5.10 As soon as reasonably practicable following the end of each day, the DCC shall, based upon the Post Commissioning Information prevailing at the end of that day, compile and

make available to each Supplier Party (via a secure electronic means for a period of at least 30 days following the day to which the report relates) a report which includes the following information in relation to Devices (other than Communications Hub Functions) listed in the Post Commissioning Information for which that Supplier Party was the Responsible Supplier on that day:

- (a) the Device ID and Device Type of each such Device;
- (b) the date on which the Post Commissioning Information for each such Device was most recently updated;
- (c) the date upon which each such Device was Commissioned; and
- (d) which of Clause 5.7 (a) and/or (b) applies in relation to each such Device.

5.11 Where requested by the Panel or the Authority, the DCC shall, as soon as reasonably practicable following any such request, provide to the Panel and/or the Authority (in an electronic format) copies of the reports referred to in Clause 5.10. Where requested by the Panel or the Authority, DCC shall additionally include in any such report the information referred to in Clause 5.8(e) in relation to each Device included in any such report.

5.12 The DCC shall ensure that each report provided under Clause 5.9, 5.10 or 5.11 is clearly marked as being “confidential”.

5.13 Where the DCC is aware that:

- (a) either or both of the steps in Clauses 5.2 (a) and/or (b) have not been carried out within 7 days following the Commissioning of a Communications Hub Function; and/or
- (b) either of Clause 5.7(a) or (b) applies in relation to a Communications Hub Function,

then the DCC shall raise an Incident in accordance with the Incident Management Policy.

5.14 Where, in relation to a Gas Proxy Function, Standalone Auxiliary Proportional Controller or a Smart Meter, a Supplier Party is aware that:

- (a) either or both of the steps in Clauses 5.3 (b) and/or (in the case of Smart Meters and Standalone Auxiliary Proportional Controllers only) 5.3(c) have not been carried out within 7 days following the Commissioning of the Device; and/or
- (b) the DCC has failed successfully to carry out the interrogation of the Device pursuant to Clause 5.4, and the Supplier has (within a period of 14 days following the Commissioning of the Device) also failed to successfully carry out the relevant interrogation,

then the Supplier Party shall not send Service Requests requesting that the DCC sends communications to that Device other than for the purposes of: (i) completing those steps; (ii) replacing the Device Security Credentials held on the Device in response to a change of supplier; or (iii) maintaining an energy supply to the relevant premises.

5.15 Where the Responsible Supplier for a Gas Proxy Function, Standalone Auxiliary Proportional Controller or Smart Meter becomes aware that the Device does not have a

recovery Trust Anchor Cell that is populated with Device Security Credentials that pertain to a DCC Recovery Certificate, then that Responsible Supplier shall (subject to Clause 5.17), as soon as reasonably practicable thereafter: other than in the case of a Gas Proxy Function, replace the Device; or, in the case of a Gas Proxy Function, replace the Communications Hub of which that Gas Proxy Function forms part.

5.16 Where a Communications Hub is returned to the DCC:

- (a) following its replacement pursuant to Clause 5.13 or 5.15; or
- (b) a Communications Hub is returned following replacement because it was not possible to interrogate the Gas Proxy Function pursuant to Clause 5.14(b),

then the Supplier Party returning the Communications Hub may (under and subject to Section F9 (Categories of Communications Hub Responsibility)) specify the reason for return as being a CH Defect.

5.17 A Responsible Supplier shall not replace a Device under Clause 5.15 where the reason that the relevant steps cannot be completed is an inability to communicate with a Device as a result of the SM WAN being unavailable.

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 48 hours 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

Managed by

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.