Department for
Energy Security
& Net Zero

Department for Energy Security & Net Zero
3-8 Whitehall Place,
London, SW1A 2EG

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

26 February 2024

Dear Colleague,

SMART METERING IMPLEMENTATION PROGRAMME: CONSULTATION ON CHANGES TO THE SMART ENERGY CODE TO ESTABLISH NEW ARRANGEMENTS FOR THE DEVICE SECURITY ASSURANCE SCHEME (KNOWN AS "CPA") AND TO PROVIDE FOR DEVICE MANUFACTURERS TO BECOME SMART ENERGY CODE (SEC) PARTIES

I invite you to respond to a consultation on changes to the main body of the Smart Energy Code (SEC) to 1) establish new arrangements for the security assurance that certain types of devices must undergo to operate on the Smart Metering Network (known as CPA). This follows the National Cyber Security Centre's (NCSC) decision to withdraw its CPA scheme for Smart Metering; 2) transitional measures to support a smooth transition to the new arrangements; 3) measures to provide for device manufacturers to become SEC parties for the purpose of becoming subscribers of IKI certificates. Further context on these measures is provided in the consultation document (Annex 1 to this letter).

The legal drafting for the proposed changes to the SEC can be found at Annexes 2 to 7. Subject to consideration of consultation responses and the Parliamentary process, the proposed changes will be introduced into the SEC using the Secretary of State's powers under section 88 of the Energy Act 2008 and are expected to take effect in late July 2024.

The consultation document provides details of how to respond. The consultation **closes on 8 April 2024.**

Yours faithfully,

Jennie Tse

Director, Smart Metering Implementation Programme

Annex 1 Consultation document
Annex 2 Proposed changes to SEC Section A (published separately)
Annex 3 Proposed changes to SEC Section F (published separately)
Annex 4 Proposed changes to SEC Section G (published separately)
Annex 5 Proposed changes to SEC Section L and SEC Appendix Q (published separately)
Annex 6 Proposed changes to SEC Appendix D (published separately)
Annex 7 Proposed changes to SEC Appendix Z (published separately)

Annex 1: Consultation document

1. General information

Why we are consulting?

The Smart Energy Code (SEC) requires electricity and gas meters, communication hubs and some other types of load control devices (that connect premises to the Smart Metering network) to undergo independent evaluation against a set of defined security characteristics to be certified under the Commercial Product Assurance (CPA) scheme. Such devices can only connect to the smart metering network if it is on the Central Product List (CPL). With the exception of Trial Devices, only devices that successfully achieve CPA Certification are placed on the CPL.[1] The National Cyber Security Centre (NCSC) currently owns and operates the CPA scheme for Smart Metering. The Department for Energy Security & Net Zero (DESNZ) has responsibility for Smart Metering.

This consultation seeks stakeholders' views on proposals to establish new arrangements for device security assurance following the NCSC decision to withdraw its CPA scheme for Smart Metering. The proposed changes also aim to put in place transitional measures to support a smooth shift to the new arrangements.

We are also proposing to change the SEC so that manufacturers who wish to become (or to remain being) a Subscriber for an IKI Certificate will need to become SEC Parties by acceding to the SEC Framework Agreement. We believe this is necessary as the SEC acts as the Subscriber Agreement between DCC and any Subscriber for a DCCKI, IKI or SMKI.

Timing

Responses to this consultation should be submitted by 5pm on 8 April 2024.

Responding to the consultation

Your response will be most useful if it is framed in direct response to the questions posed, by reference to our numbering, though further comments and evidence are also welcome.

Responses should be submitted to smartmetering@energysecurity.gov.uk

When responding, please state whether you are responding as an individual or representing the views of an organisation.

Confidentiality and data protection

Information you provide in response to this consultation, including personal information, may be disclosed in accordance with UK legislation (the Freedom of Information Act 2000, the Data Protection Act 2018, and the Environmental Information Regulations 2004).

[1] In 2012, DESNZ' predecessor DECC, selected NCSC's CPA scheme to provide device security assurance. The scheme is designed to assure certain smart metering hardware with a specific firmware version and includes an assurance maintenance process that also allows for updating firmware versions under the same certificate.

If you want the information that you provide to be treated as confidential, please tell us but be aware that we cannot guarantee confidentiality in all circumstances. An automatic confidentiality disclaimer generated by your IT system will not be regarded by us as a confidentiality request.

We will process your personal data in accordance with all applicable data protection laws. See our privacy policy.

We will summarise all responses and publish this summary on the SEC website. The summary will include a list of names or organisations that responded, but not people's personal names, addresses or other contact details.

Territorial extent

This consultation applies to the gas and electricity markets in Great Britain. Responsibility for energy markets in Northern Ireland lies with the Northern Ireland Executive's Department for the Economy.

Quality assurance

This consultation has been carried out in accordance with the government's consultation principles.

If you have any complaints about the way this consultation has been conducted, please email the Better Regulation Unit on bru@energysecurity.gov.uk at the Department for Energy Security & Net Zero.

2. New Device Security Assurance (CPA) Scheme

The Need to Establish New Device Assurance Arrangements

1. In its White Paper "The future of NCSC Technology Assurance", published in September 20212, the NCSC set out its approach to address the challenges the UK faces for Technology Assurance both now and in the future. Amongst a range of measures designed to support their new approach, NCSC informed DESNZ, as the Government Department with responsibility for Smart Metering, of its intention not to continue to provide the CPA assurance scheme for Smart Metering. This followed its 2020 decision to close the CPA scheme for all other types of technology.
2. Consequently, there is a need to implement new arrangements for device security assurance, and specifically to provide for a new device assurance scheme operator to replace the roles which are currently fulfilled by NCSC. NCSC remains actively supportive of the requirement for smart metering device assurance. As set out later in this document, NCSC will continue to accredit laboratories participating in the new scheme and support a smooth transition to the new arrangements. NCSC will also remain available to provide security advice upon request to SSC and DESNZ should this be required.

3. The proposals set out in this document enable the new arrangements to be established and have been developed in cooperation with NCSC. They are also designed to be consistent with enduring security governance responsibilities for Smart Metering.

Overview of proposed new device assurance arrangements

4. The Security Sub-Committee (SSC) of the SEC Panel is currently accountable for security aspects which include carrying out end-to-end Risk Assessments and maintenance of the Security Architecture as defined in the SEC (G7.19/20). Under the proposals that are subject to this consultation, the responsibility for CPA scheme ownership will transfer from NCSC to the SSC. The SSC would take on overall responsibility for the delivery, operation, and maintenance of the scheme, which would continue to be referred to as the 'CPA Scheme', and the relevant SEC obligations applying to CPA Certification would continue. This arrangement would broadly align responsibilities and arrangements for device security assurance with those that are already in place for DCC User security assessments[3].

5. A summary of the proposed roles and responsibilities under the proposed new arrangements is set out below:

    - **Scheme Sponsor:** DESNZ will continue to be the CPA Scheme Sponsor and maintain overall accountability for ensuring that risks associated with UK critical national infrastructure (CNI) in relation to Smart Metering are appropriately managed as part of the end-to-end Smart Metering System.

[2] https://www.ncsc.gov.uk/collection/technology-assurance/future-technology-assurance

[3] To use the Data Communications Company (DCC) systems, all SEC Parties must undertake a User Security Assessment conducted by the User Competent Independent Organisation (CIO).

- **Scheme Owner (SOwn):** The SSC will become the "Scheme Owner" with responsibility transferring from NCSC. SSC will have overall responsibility for the delivery, operation, and maintenance of the CPA Scheme, and the relevant obligations applying to CPA Certification will continue.

- **Scheme Operator (SOp):** The SCC will also take on responsibility to procure and appoint a Scheme Operator to replace NCSC. The Scheme Operator will establish a technically expert Evaluation Team to conduct device evaluations, which is a task that NCSC currently performs. The Scheme Operator will also establish a day-to-day administration and management function for devices being evaluated. This will review recommendations from Test Labs and award CPA Certificates, as appropriate. In the transition to the new arrangements, it is proposed that NCSC's current evaluators will maintain some oversight and support the new Evaluation Team.

- **Test Labs:** Test Labs will continue to be accredited by NCSC who is currently building a community of industry-based labs, "Cyber Resilient Test Facilities (CRTFs)", which can provide independent assessment of a range of technologies. Based on initial discussions with NCSC, we are expecting that these accredited Test Labs will also be appropriate for evaluating smart metering devices against the CPA Security Characteristics. SSC will be responsible for ensuring that Test Labs are suitable to perform CPA assurance for Smart Metering in line with their published CPA Policies and Procedures document.

6. Currently the responsibility for updating and managing the existing CPA Security Characteristics over time is shared between SSC and NCSC. As part of our changes, we are proposing that this will become the sole responsibility of the SSC with smart metering devices continuing to need to demonstrate compliance with the CPA Security Characteristics.

7. The Risk Review process, which periodically reviews if existing CPA certified devices should retain their CPA certificate, will continue with responsibility for its operation transferring from the NCSC to the new Scheme Owner.

8. Manufacturers will still nominate their preferred Test lab but there will be changes to how test labs are contracted for their CPA work:
   - Test labs will be retained by the SOp on a framework agreement.
   - To provide central oversight and improve operational efficiency and cost effectiveness, individual contract or work orders placed per device by the manufacturers will be with the SOp rather than directly with the Test Lab which is currently the case.
   - The testing fees will be paid by the manufacturer to the SOp who will in turn, pay the Test Lab.
   - Payment terms and milestones will be aligned where possible to maintain the integrity of the process.
   - The manufacturer's commercial relationship will be with the SOp.
   - The manufacturer will still have a direct working relationship with the Test Lab to develop the testing plan and execute the tests, as is common practice out of necessity in the case of any software or hardware testing.
   - Manufacturers wishing to obtain CPA Certification for their device, will approach the SOp rather than approaching a Test Lab directly as happens now.
   - The SOp will review evaluations from an NCSC accredited Test Lab and award a CPA Certificate as appropriate.

Transitional Arrangements.

9. Transitional arrangements will be necessary to support the implementation of the new CPA scheme. NCSC will continue the current arrangements through a transition period until the new arrangements are in place and have bedded in. It is also planned that, once the new scheme is operating, there will be a period of handover and possible parallel running to allow a smooth transition away from NCSC's current responsibilities under the existing CPA Scheme and, where possible, the completion of any ongoing smart metering device evaluations.

Proposed Amendments

DCC Licence conditions

10. As currently drafted, DCC Licence Condition 22.22 contains broad provisions covering matters that relate to security and to financial liabilities that SEC Parties may expect to incur while operating in line with the SEC. We believe the provisions sufficiently cover the proposed revised arrangements, and so we are not proposing any changes to this or any other DCC Licence Condition, nor do we believe that any changes to supply licences are needed.

Smart Energy Code (SEC)

11. We are proposing to amend SEC Section G7.20 to place a new obligation on the SSC to ensure that CPA Scheme Operator services, are both suitable in nature and sufficient in quantity to meet the reasonable requirements of the CPA Scheme, at all times. Such services will be required to comply with the relevant requirements as specified in a proposed new SEC Section G.13, which we deal with below.

12. At SEC Section G7.19 we are proposing to define a set of new consequential duties for the SSC which include (as required) maintaining and developing the:
    - Existing CPA Security Characteristics for smart metering devices to ensure that any new smart metering devices could be captured within scope (as required),
    - New "CPA Policies and Procedures" document, which sets out the arrangements relating to the evaluation of smart metering devices and procedures that smart metering device manufacturers must follow to obtain and maintain CPA Certification; and the
    - New "CPA Assurance Maintenance Plan", which will identify the components in smart metering devices that will require new CPA certification if their technical specifications change.

13. As highlighted previously, we are also proposing to introduce a new SEC Section G.13 to set out the requirements that the CPA Scheme Operator must meet and obligations on the SSC in relation to managing the role of the CPA Scheme Operator. This includes:
    - Managing the procurement, appointment, and activity scope of the CPA Scheme Operator
    - Ensuring the CPA Scheme Operator's Compliance with the SEC
    - The CPA Scheme Operator's performance and operational independence
    - Ensuring the CPA Scheme Operator has sufficient capacity to meet reasonable demands for CPA assurance from smart metering device manufacturers.

14. To do so, the CPA Scheme Operator will be required to develop and manage (as required) the new "CPA Test Lab Framework Agreement" that will govern the revised contractual relations between the CPA Scheme Operator, smart metering device manufacturers, and CPA Test Labs, including these labs' performance of functions relating to the revised CPA Scheme. For consistency with the existing SEC rules, the rules in the new SEC Section G.13 were modelled on those for managing the User Independent Security Assurance Service Provider role, as set out in SEC Section G8.1.

15. To support a timely, efficient, and effective transfer to the proposed revised CPA scheme from NCSC's responsibilities under the current CPA Scheme, we are proposing to introduce the new SEC Section G.14. This will provide for a new "CPA Transition Approach Document", which will set out the arrangement necessary to support the transition to, and entry into full effect of, the revised CPA scheme provisions. We aim to consult on the CPA Transition Approach Document in due course. Its initial version is likely to be used to switch off the main changes but may keep active some of the proposed changes to SEC Section G that are necessary to begin the transition period. This may include activities, such as enabling the appointment of the CPA Scheme Operator. Other activities, such as the final transfer of responsibilities from NCSC to the new scheme operator will not become active until such time as they are ready to be fully implemented.

16. SEC Section F covers the rules relating to CPA Certificates. Valid CPA Certificates that have been issued through the current CPA Scheme will remain valid, unless those CPA Certificates have expired, been withdrawn, or are cancelled. To reflect this, and the new CPA Scheme Operator's role in administering CPA Certificates, we are proposing small consequential changes to replace "NCSC" with "CPA Scheme Operator", in SEC Section F and SEC Appendix Z (CPL Requirements Document).

17. For consistency, and to avoid confusion, we propose to update SEC Section A with definitions of the new documents that are being proposed in section 10 of this consultation to SEC Section G7.19, G.20 and in the new SEC Section G.13 and G.14,. We are also proposing to correct a typographical error in SEC Section G9.12.

18. Subject to considering responses to this consultation and the Parliamentary process, we will introduce the proposed changes into the SEC using the Secretary of State's powers under Energy Act 2008 (Section 88) and expect the changes to take effect in late July 2024.

Consultation Questions

	Consultation questions
1.	Do you have any comments on the principles of the proposed changes to device security assurance as set out in this consultation?
2.	Do you have any comments on the legal drafting of main-body SEC in Annexes 2 to 7?
3.	Do you have any comments on the timing of making the proposed changes to the SEC?

3. Manufacturers as SEC Parties

Manufacturers holding SMKI Certificates

19. In summer 2023, changes were made to the SEC via Modification Proposal 168 to permit device Manufacturers to become subscribers for IKI Certificates so that the associated Private Key can be used to sign requests for firmware images to be associated with a Device Model on the Central Products List (CPL) and allowing the Panel to check this signature using the Public Key in the IKI Certificate. The change also noted that manufacturers would need access to the Certificate Revocation List.

20. The changes did not, however, require manufacturers to become SEC Parties for such purposes. Government believes that this was an omission since the SEC acts as the Subscriber Agreement between DCC and any subscriber for a DCCKI, IKI or SMKI Certificate, in addition to acting as the Relying Party Agreement for these PKIs[4]. Subscriber Agreements and Relying Party Agreements are standard contractual documents of Public Key Infrastructures and Government believes that it is important that Manufacturers are contractually subject to these provisions when acting as a subscriber or relying party. Consequently, we are proposing that Manufacturers who aren't already SEC Parties and who wish to become (or to remain being) a Subscriber for an IKI Certificate will need to become SEC Parties by acceding to the SEC Framework Agreement.

21. Manufacturers who have already become subscribers by virtue of the changes made using MP168, but who are not currently SEC Parties would also have to acknowledge that the provisions of the SEC apply to them in relation to any certificate that was issued prior to becoming a SEC Party. Where such a manufacturer does not become a SEC Party within 6 months of the changes being made to the SEC, the DCC will be required to revoke any certificates issued to them.

22. As part of this change, we are also proposing that Security Sub-Committee (SSC) membership be amended to include representation from a Manufacturer Party. Furthermore, we are proposing a new obligation on Manufacturers to notify the SSC of any material security vulnerabilities that it becomes aware of in respect of any Devices for which it is the Manufacturer, which is commensurate with obligations on other SEC Parties.

Proposed Amendments

23. To reflect our proposals to require smart metering device manufacturers to become SEC Parties, we are proposing modifications to SEC Section G7.3 and SEC Section G7.14 and to include a new SEC Section G13.A and new SEC Section 13.B. The modifications and additions include provisions to enable smart metering device Manufacturers to be represented on the Security Sub-Committee (SSC) and for their conduct and accountability to be aligned with the existing SEC rules relating to appointments to the SSC. For consistency with SEC Party obligations, the proposal for manufacturers to become SEC Parties will also introduce a new SEC Section G3.21A, which obligates manufacturers to notify the SSC of any significant security vulnerability in, or likely significant negative impact from, any smart metering device, which they produced.

[4] See for example the Subscriber Obligations in SEC Section L11 and the Relying Party Obligations in Section L12, as well as the limitation of liability provisions in Section M.

24. We also propose several consequential changes to SEC Section L3.20, which covers IKI Certificates, SEC Appendix D (SMKI Registration Authority Policies and Procedures) and to SEC Appendix Q (IKI Certificate Policy) by removing any references to “Manufacturer” as the documents can adequately refer to smart metering device manufacturers as “Parties” and by clarifying that manufacturers are referred to as SEC Parties in SEC Appendix Z (CPL Requirements Document).

Consultation Questions

Consultation questions	
1.	Do you have any comments on the principles of the proposed changes to the main body SEC to allow manufacturers to become SEC Parties.
2.	Do you have any comments on the legal drafting for the main-body SEC changes in Annexes 4 to 7?

4. Next steps

25. This consultation will remain open until 5pm on 8 April 2024. Once it has closed, we will review the comments submitted in response to the consultation and will aim to publish our conclusions around the end of April 2024.

26. We are then proposing to make the changes to the main-body SEC in Q3 2024 using powers conferred on the Secretary of State under section 88 of the Energy Act 2008. To the extent that any changes need to be disapplied until the new arrangements are operating and transition is complete, the CPA Transition Approach Document will be used for disapplying the necessary provisions. We will consult on the initial CPA Transition Approach Document in due course. Any further revisions to the CPA Transition Approach Document will be consulted on by the SSC as transition progresses.

CPA Assurance Maintenance Plan	has the meaning given to that expression in Section G7.19(h) (Document Development and Maintenance). ~~means the document agreed with the NCSC that describes the components of a device which, if changed, will require a new CPA Certificate to be issued.~~
CPA Certificate~~s~~	~~has the meaning given to that expression in Section F2.4 (Background to Assurance Certificates).~~ means an Assurance Certificate issued for the purposes of the CPA Scheme by: (a) prior to the commencement of the Revised CPA Arrangements, the NCSC; or (b) following the commencement of the Revised CPA Arrangements, the CPA Scheme Operator.
CPA Policies and Procedures	has the meaning given to that expression in Section G7.19(g) (Document Development and Maintenance).
CPA Scheme	means the Commercial Product Assurance Scheme in relation to Devices for the purposes of the Code, being a scheme described in the CPA Policies and Procedures under which the security of those Devices is required to be assured by the application for and issuing of CPA Certificates.
CPA Scheme Operator	has the meaning given to that expression in Section G13.1 (Procurement of the CPA Scheme Operator).
CPA Scheme Operator Services	has the meaning given to that expression in Section G13.3 (Scope of CPA Scheme Operator Services).

CPA Security Characteristics	means the documents maintained by the Security Sub-Committee ~~published from time to time on the NCSC website~~ that set out the features, evaluation criteria and deployment requirements necessary for a Manufacturer to obtain a CPA Certificate in respect of a Device Model of one or more of the following: (a) 'Gas Smart Metering Equipment'; (b) 'Electricity Smart Metering Equipment'; (c) 'Communications Hubs'; (d) 'HAN Connected Auxiliary Load Control Switches'; (e) Standalone Auxiliary Proportional Controllers; (f) any such other Device as may from time to time be specified by the Security Sub-Committee as requiring a CPA Certificate.
CPA Test Lab	means a Test Lab which meets the criteria specified in the CPA Policies and Procedures for performing the functions of a testing laboratory for the purposes of the CPA Scheme.
CPA Test Lab Framework Agreement	has the meaning given to that expression in Section G13.3(b) (Scope of CPA Scheme Operator Services).
CPA Transition Approach Document	means the SEC Subsidiary Document of that name to be developed pursuant to Section G14 (CPA Transition Document).
Manufacturer Party	means a Manufacturer which is a Party to this Code.

Revised CPA Arrangements	has the meaning given to that expression in Section G14.4 (Definitions).
Security Sub-Committee (Manufacturer Party) Member	has the meaning given to that expression in Section G7.13A (Membership of the Security Sub-Committee).
SSC Guidance for Device Security Assurance and Triage	means the document of that name developed by the SSC in accordance with Section G7.19(~~g~~i).
Test Lab	means a testing laboratory accredited by the NCSC.
Triage	has the meaning given to that expression in Section G12.9 (Definitions).

Note: All definitions shown in clean text are new additions to Section A. Definitions shown in change track are existing definitions being amended.

F2. CENTRAL PRODUCTS LIST

Central Products List

F2.1 The Panel shall establish and maintain a list (the "Central Products List") of:

(a) the SMETS2+ Device Models for which the Panel has received all the Assurance Certificates required for the Physical Device Type relevant to that Device Model (known as the Certified Products List); and

(b) in the case of SMETS1 Device Models, those Device Models for which the Panel has received all the information required in accordance with the CPL Requirements Document (which does not require any certification of SMETS1 Devices under the CPA or any other assurance scheme).

F2.2 The Panel shall ensure that the Central Products List identifies the Data required in accordance with the CPL Requirements Document, and that the Central Products List is updated to add and remove Device Models in accordance with the CPL Requirements Document (including as described in Section F2.7A).

F2.2A Where a Party disagrees with any decision of the Panel to add, remove, not remove, reinstate, or not reinstate a SMETS1 Device Model to or from the Central Products List, that Party may refer the matter to the Authority for its determination, which shall be final and binding for the purposes of this Code.

Background to Assurance Certificates

F2.2B For SMETS1 Device Models, there are no required Assurance Certificates for any of the Physical Device Types.

F2.3 The Technical Specification relevant to the Physical Device Type sets out which Physical Device Types require Assurance Certificates from one or more of the following persons (each being an “Assurance Certification Body”):

(a) the ZigBee Alliance;

(b) the DLMS User Association; and

(c) ~~NCSC~~the CPA Scheme Operator.

F2.4 The following Assurance Certification Bodies issue the following certificates in respect of Device Models of the relevant Physical Device Types (each being, as further described in the applicable Technical Specification, an "Assurance Certificate"):

(a) the ZigBee Alliance issues certificates which contain the ZigBee certified logo and interoperability icons;

(b) the DLMS User Association issues certificates which include the conformance tested service mark ("DLMS Certificates"); and

(c) ~~NCSC~~the CPA Scheme Operator issues commercial product assurance scheme certificates ("CPA Certificates").

F2.5 An Assurance Certificate will not be valid unless it expressly identifies the Device Model(s) and the relevant Physical Device Type to which it applies. With the exception of a CPA Certificate, an Assurance Certificate will not be valid if it specifies an expiry date that falls more than 6 years after its issue.

Expiry and renewal of CPA Certificates

F2.6 As CPA Certificates that have not been withdrawn or cancelled will require periodic renewal at their expiry or renewal date, the following Parties shall ensure that action is taken to ensure that a CPA Certificate can be considered for renewal in respect of Device Models for the following Physical Device Types before the expiry or renewal date of such CPA Certificate (to the extent Device Models of the relevant Physical Device Type require CPA Certificates in accordance with the applicable Technical Specification):

(a) the DCC for Communications Hubs; and

(b) the Import Supplier and/or Gas Supplier (as applicable) for Device Models of all other Physical Device Types.

F2.7 The Panel shall notify the Parties on or around the dates occurring 12 and 6 months prior to the date on which the CPA Certificate for any Device Model is due to expire. The Panel shall also provide to the Parties any notice concerning CPA Certificates which the ~~NCSC~~Security Sub-Committee asks the Panel to provide to the Parties.

Consequence of Expiry, Withdrawal or Cancellation of Assurance Certificates

F2.7A Where:

(a) a CPA Certificate for a Device Model expires or is not renewed or is withdrawn or cancelled by the ~~NCSC~~CPA Scheme Operator, then the Security Sub-Committee shall determine whether to remove that Device Model from the Central Products List in accordance with the CPL Requirements Document, which may provide for a CPA Certificate Remedial Plan to be imposed;

(b) any other type of Assurance Certificate for a Device Model is withdrawn or cancelled by the Assurance Certification Body that issued the certificate, then the Panel shall remove that Device Model from the Central Products List.

F2.7B Where a Party disagrees with any decision of the Security Sub-Committee made in accordance with the CPL Requirements Document:

(a) to remove or not remove a Device Model from the Central Products List;

(b) to not approve the Party's CPA Certificate Remedial Plan (where the Security Sub-Committee has determined that a CPA Certificate Remedial Plan is to be imposed on the Party), that Party may refer the matter to the Authority for its determination, which shall be final and binding for the purposes of this Code.

Publication and Use by the DCC

F2.8 Subject to the requirements of the CPL Requirements Document, the Panel shall (within one Working Day after being required to add or remove Device Models to or from the Central Products List in accordance with the CPL Requirements Document):

(a) provide the updated Central Products List to the DCC (by way of an extract containing such subset of the information contained within the Central Products List as the DCC reasonably requires from time to time);

(b) publish a copy of the updated Central Products List on the Website; and

(c) notify the Parties that the Central Products List has been updated.

F2.9 Subject to the requirements of the CPL Requirements Document, the DCC shall, from time to time, use and rely upon the Central Products List most recently received by the DCC from the Panel at that time, provided that the DCC shall be allowed up to 24 hours from receipt to make any modifications to the Smart Metering Inventory that are necessary to reflect the updated Central Products List.

Deployed Products List

F2.10 The DCC shall create, keep reasonably up-to-date and provide to the Panel (and the Panel shall publish on the Website) a list (the "Deployed Products List") of all the combinations of different Device Models that comprise a Smart Metering System (together with Associated Type 2 Devices) that exist from time to time (to the extent recorded by the Smart Metering Inventory).

SMETS1 Lists

F2.10A The DCC shall create, keep up-to-date and provide to the Panel (and the Panel shall publish on the Website) lists of:

(a) each combination of SMETS1 Device Models and communication services provider in relation to which the DCC has demonstrated through testing (which may include testing of a different combination that the DCC considers to be substantively equivalent) that it is able to successfully process SMETS1 Service Requests and relevant SMETS1 Alerts (the "SMETS1 Eligible Product Combinations"), including the date on which each entry was first added to the list; and

(b) each combination of SMETS1 Device Models and communication services provider) in relation to which the DCC is at that time:

(i) considering whether testing or development is required to demonstrate the capability; or

(ii) developing and/or testing the capability,

to successfully process SMETS1 Service Requests and relevant SMETS1 Alerts (the "SMETS1 Pending Product Combinations"), provided that the DCC shall

not add a Device Model combination to the SMETS1 Pending Product Combinations where the relevant Testing Participant has indicated pursuant to clause 9 (SMETS1 Pending Product Combinations Tests) of the Enduring Testing Approach Document that such information should be treated as confidential.

F2.10B The obligation of the DCC under Section F2.10A(a) shall only apply once the DCC is first permitted under the Transition and Migration Approach Document to add a combination of Device Models to the SMETS1 Eligible Product Combinations.

Technical Specification Incompatibility

F2.11 The Panel shall create, keep reasonably up-to-date and publish on the Website a matrix specifying:

(a) which Versions of each Technical Specification are incompatible with which Versions of each other Technical Specification; and

(b) where applicable, those areas in respect of which the Version of the Technical Specification is not incompatible with the Version of the other Technical Specification but may be subject to the application of particular constraints as identified.

F2.12 For the purposes of Section F2.11:

(a) 'incompatible' means in respect of a Version of any Technical Specification, that Devices or apparatus which comply with that Version are known to have been designed in a manner that does not enable them to inter-operate fully with Devices or apparatus that comply with the specified Version of each other Technical Specification;

(b) each reference to a Version of a Technical Specification shall be read as being to that Version taken together with any relevant Version of the GB Companion Specification (as identified in the TS Applicability Tables), so that if there is more than one relevant Version of the GB Companion Specification for any Version of a Technical Specification, the matrix shall make separate provision for each of them; and

(c) the matrix need not specify:

(i) which Versions of the ESMETS are incompatible with Versions of the GSMETS;

(ii) which Versions of the GSMETS are incompatible with which Versions of:

(A) the ESMETS;

(B) the HCALCSTS; or

(C) the SAPCTS.

F2.13 The Panel shall, as soon as reasonably practicable after it makes a change to such matrix, notify all the Parties that a change has been made.

Firmware Information Repository

F2.14 The Panel shall establish and maintain a list of firmware releases, updates, and corresponding Manufacturer contact details (the "Firmware Information Repository").

F2.15 The Panel shall ensure that the Firmware Information Repository contains a minimum of three fields:

(a) a number which uniquely identifies a record on the Central Products List, which is a mandatory field;

(b) Manufacturer contact details, which is a mandatory field, to include email address, telephone number and business address; and

(c) a free text field for release notes that Manufacturers can record against, which is a mandatory field for completion but the content is at the discretion of the Manufacturers.

F2.16 The Firmware Information Repository will be updated alongside the Central Products List, with the number which uniquely identifies a record on the Central Products List providing a cross reference.

F2.17 The Party or any other person submitting Device details for addition to the Central Products List shall also supply the details listed in F2.15 for the same Device.

Device Trials

F2.18 The Security Sub-Committee shall consider applications from Manufacturers for SMETS2+ Device Models to be added to the Central Products List, on a limited trial basis, without a CPA Certificate needing to be issued by the ~~NCSC~~CPA Scheme Operator. If approved by the Security Sub-Committee, the relevant SMETS2+ Device Model will be known as a "Trial Device Model" for the duration set out in the approval (the "Trial Device Approval"). The Security Sub-Committee shall have sole discretion in deciding whether to grant a Trial Device Approval.

F2.19 In its application for Trial Device Approval, the applicant Manufacturer must evidence that the SMETS2+ Device Model for which it is seeking approval has all Assurance Certificates other than a CPA Certificate issued by the ~~NCSC~~CPA Scheme Operator.

F2.20 The Security Sub-Committee shall require a business rationale to support the application, a security risk assessment, and assurance that Energy Consumers of Trial Device Models shall be required to opt into trial participation and informed of the implications of doing so, and may (at its sole discretion) set additional requirements that must be evidenced in an application.

F2.21 Where a Trial Device Approval is granted, the Security Sub-Committee shall set out in a written notice to the Manufacturer and the Panel:

(a) a detailed description of the Trial Device Model;

(b) a summary of why the Trial Device Approval is being granted and the assessment undertaken by the Security Sub-Committee in considering the application;

(c) the start date and expiry date of the Trial Device Approval;

(d) the maximum number of Devices of the Trial Device Model that may be deployed; and

(e) any other conditions applied to the Trial Device Approval.

F2.22 The Security Sub-Committee shall determine the appropriate level of detail to be provided in the Trial Device Approval notice and shall not be required to disclose any information it considers sensitive.

F2.23 If one or more of the conditions applicable to the Trial Device Model are breached, then the Trial Device Approval may be withdrawn or cancelled by the Security Sub-Committee.

F2.24 Where an application is not approved, the Security Sub-Committee shall set out in a written notice to the Manufacturer and the Panel a summary of why approval has not been granted and the assessment undertaken in considering the application. The Security Sub-Committee shall determine the appropriate level of detail to be provided in the summary and shall not be required to disclose any information it considers sensitive.

F2.25 A Trial Device Model will be deemed to have a valid CPA Certificate for the duration of the Trial Device Approval. The Security Sub-Committee shall issue a trial certificate (the "Trial Device Certificate") for the duration of the trial in lieu of the CPA Certificate that would ordinarily be issued by the ~~NCSC~~CPA Scheme Operator. The Trial Device Certificate will include an identifier code which is unique to the Trial Device Model and the Trial Device Approval as well as an expiry date which matches the expiry date of the Trial Device Approval. The Trial Device Certificate will be provided to the Manufacturer and the Panel.

F2.26 In respect of a Trial Device Model, this Code will be construed such that any requirement for a SMETS2+ Device Model to have a CPA Certificate shall be deemed satisfied by a valid Trial Device Certificate. Where necessary, the requirements of this Code applicable to a CPA Certificate will be construed so as to not inhibit the use of a Trial Device Model in accordance with a Trial Device Approval and Sections F2.18 to F2.32.

F2.27 With effect from the start date set out in the Trial Device Approval, the Panel shall add the Trial Device Model to the Central Products List. The Central Products List must show that the relevant SMETS2+ Device Model is a Trial Device Model, identify

the specific Trial Device Approval that applies to the Trial Device Model, and include the expiry date for such approval.

F2.28 On a monthly basis, the DCC shall provide the Security Sub-Committee with a copy of the Smart Metering Inventory so that the Security Sub-Committee can extract details of Trial Device Models.

F2.29 The Manufacturer of a Trial Device Model may apply to the Security Sub-Committee to request an amendment to its Trial Device Approval. The Security Sub-Committee may amend a Trial Device Approval at any time and at its sole discretion, irrespective of whether an amendment application has been made by the Manufacturer. If the Security Sub-Committee amends a Trial Device Approval, it shall notify the Manufacturer and the Panel. The notice will include a summary of why the Trial Device Approval has been amended. The Security Sub-Committee shall determine the appropriate level of detail to be provided and shall not be required to disclose any information it considers sensitive. Where necessary, the Panel shall update the Central Products List to reflect such amendment.

F2.30 The Security Sub-Committee may withdraw or cancel a Trial Device Approval at any time and at its sole discretion. Upon such withdrawal or cancellation, the Security Sub-Committee shall notify the Manufacturer and the Panel. The notice will include a summary of why the Trial Device Approval has been withdrawn or cancelled. The Security Sub-Committee shall determine the appropriate level of detail to be provided and shall not be required to disclose any information it considers sensitive.

F2.31 If a Trial Device Approval expires, or is withdrawn or cancelled, the Trial Device Certificate will expire, be withdrawn or be cancelled (as applicable) by the Security Sub-Committee and the provisions of Clause 6 (Removal of Device Models from the List) of Appendix Z shall apply in determining whether or not to remove the Trial Device Model from the Central Products List and whether a Trial Device Remedial Plan is to be imposed. If it is determined that the Trial Device Model shall be removed from the Central Products List, the Manufacturer may either apply for a new Trial Device Approval or apply for a CPA Certificate.

F2.32 Where a Trial Device Model is removed from the Central Products List, all Devices of the relevant SMETS2+ Device Model must be promptly Decommissioned by the Responsible Supplier, unless:

(a) the relevant SMETS2+ Device Model has since gained a CPA Certificate (or a new Trial Device Certificate) and has been updated accordingly on the Central Products List; or

(b) the relevant Device can be (and is) updated via firmware to become a SMETS2+ Device Model which is listed on the Central Products List.

SECTION G - SECURITY

G3 SYSTEM SECURITY: OBLIGATIONS ON USERS

Unauthorised Activities: Duties to Detect and Respond

G3.1 Each User shall:

(a) take reasonable steps to ensure that:

(i) its User Systems are capable of identifying any deviation from their expected configuration; and

(ii) any such identified deviation is rectified; and

(b) for these purposes maintain at all times an up-to-date list of all hardware, and of all software and firmware versions and patches, which form part of the configuration of those User Systems.

G3.2 Each User shall take reasonable steps:

(a) to ensure that its User Systems are capable of detecting any unauthorised software that has been installed or executed on them and any unauthorised attempt to install or execute software on them;

(b) if those User Systems detect any such software or such attempt to install or execute software, to ensure that the installation or execution of that software is prevented; and

(c) where any such software has been installed or executed, to take appropriate remedial action.

G3.3 Each User shall:

(a) ensure that its User Systems record all attempts to access resources, or Data held, on them;

(b) ensure that its User Systems detect any attempt by any person to access resources, or Data held, on them without possessing the authorisation required

to do so; and

(c) take reasonable steps to ensure that its User Systems prevent any such attempt at unauthorised access.

Security Incident Management

G3.4 Each User shall ensure that, on the detection of any unauthorised event of the type referred to at Sections G3.1 to G3.3, it takes all of the steps required by its User Information Security Management System.

G3.5 Each User shall, on the occurrence of a Major Security Incident in relation to its User Systems, ensure that the Panel and the Security Sub-Committee are promptly notified.

System Design and Operation

G3.6 Each User shall, at each stage of the System Development Lifecycle, have regard to the need to design and operate its User Systems so as to protect them from being Compromised.

Management of Vulnerabilities

G3.7 Each Supplier Party shall ensure that either a tester who has achieved CREST certification or an organisation which is a CHECK service provider carries out assessments that are designed to identify any vulnerability of its User Systems to Compromise:

(a) in respect of each of its User Systems, on at least an annual basis;

(b) in respect of each new or materially changed component or functionality of its User Systems, prior to that component or functionality becoming operational; and

(c) on the occurrence of any Major Security Incident in relation to its User Systems.

G3.8 Each User shall ensure that it carries out assessments that are designed to identify any vulnerability of its User Systems to Compromise:

(a) in respect of each of its User Systems, on at least an annual basis;

(b) in respect of each new or materially changed component or functionality of its User Systems, prior to that component or functionality becoming operational; and

on the occurrence of any Major Security Incident in relation to its User Systems.

G3.9 Each User shall ensure that:

(a) in respect of any new or materially changed component or functionality of its User Systems which comprises (or includes) a System that is being incorporated into its User Systems for the first time:

(i) it notifies the Security Sub-Committee prior to that System becoming an operational part of its User Systems;

(ii) together with that notification it provides to the Security Sub-Committee an adequate description of the System, of the purpose for which it will be used, and of the nature of its relationship to the other component parts of the User Systems; and

(iii) that System does not become an operational part of its User Systems unless and until the Security Sub-Committee has authorised the User to bring it into operation (for which purpose, following any such review or assessment as it may consider appropriate, the Security Sub-Committee shall be entitled to give or withhold authorisation by means of notice to the User); and

(b) where, following any assessment of its User Systems in accordance with Section G3.7 or G3.8, any material vulnerability has been detected, a User shall ensure that it:

(i) takes reasonable steps to ensure that the cause of the vulnerability is rectified, or the potential impact of the vulnerability is mitigated, as soon as is reasonably practicable;

(ii) promptly notifies the Security Sub-Committee of the steps being taken to rectify its cause or mitigate its potential impact (as the case may be) and the time within which they are intended to be completed; and

(c) where a material component or material functionality of its User Systems is being discontinued or where a User System is being decommissioned;

(i) the User notifies the Security Sub-Committee prior to the component or functionality being discontinued or the User System being decommissioned (as relevant);

(ii) together with that notification, the User provides to the Security Sub-Committee an adequate description of the reason for the change and the proposed timing of the change;

(iii) the discontinuation or decommissioning is not undertaken before the Security Sub-Committee has been notified; and

(iv) the User takes any reasonable action advised by the Security Sub-Committee.

Management of Data

G3.10 Each User shall:

(a) develop and maintain, and hold all Data in accordance with, a User Data Retention Policy; and

(b) when any Data held by it cease to be retained in accordance with the User Data Retention Policy, ensure that they are securely deleted in accordance with its Information Classification Scheme.

User Systems: Duty to Separate

G3.11 Each User shall take reasonable steps to ensure that any software or firmware that is installed on its User Systems for the purposes of security is Separated from any software or firmware that is installed on those Systems for any other purpose.

User Systems: Independence of DCC Live Systems

G3.12 Each User shall ensure that no individual is engaged in:

(a) the development of bespoke software or firmware, or the customisation of any software or firmware, for the purpose of its installation on any part of its User

Systems; or

(b) the development, design, build, testing, configuration, implementation, operation, maintenance, modification or decommissioning of any part of its User Systems,

unless that individual satisfies the requirements of Section G3.13.

G3.13 An individual satisfies the requirements of this Section only if, at any time at which that individual is engaged in any activity described in Section G3.12, he or she:

(a) is not at the same time also engaged in:

(i) the development of bespoke software or firmware, or the customisation of any software or firmware, for the purpose of its installation on any part of the DCC Live Systems; or

(ii) the development, design, build, testing, configuration, implementation, operation, maintenance, modification or decommissioning of any part of the DCC Live Systems; and

(b) has not been engaged in any activity described in paragraph (a) for a period of time which the User reasonably considers to be appropriate, having regard to the need to ensure the management of risk in accordance with its User Information Security Management System.

G3.14 Each User shall ensure that no resources which form part of its User Systems also form part of the DCC Live Systems.

Monitoring

G3.15 Each Supplier Party shall take reasonable steps to ensure that its User Systems are capable of detecting Anomalous Events, in particular by reference to the:

(a) sending or receipt (as the case may be) of Service Requests, Pre-Commands, Signed Pre-Commands, Service Responses and Alerts;

(b) audit logs of each Device for which it is the Responsible Supplier; and

(c) error messages generated by each Device for which it is the Responsible

Supplier.

G3.16 Each Supplier Party shall:

(a) take reasonable steps to ensure that its User Systems detect all Anomalous Events; and

(b) ensure that, on the detection by its User Systems of any Anomalous Event, it takes all of the steps required by its User Information Security Management System.

Manufacturers: Duty to Notify and Be Notified

G3.17 Where a User becomes aware of any material security vulnerability in, or likely cause of a material adverse effect on the security of:

(a) any hardware, software or firmware which forms part of its User Systems; or

(b) (where applicable) any Smart Metering System (excluding a Communications Hub Function or Gas Proxy Function which forms part of a SMETS2+ Device) for which it is the Responsible Supplier,

it shall comply with the requirements of Section G3.18.

G3.18 The requirements of this Section are that the User shall:

(a) wherever it is reasonably practicable to do so notify the manufacturer of the hardware or Device or the developer of the software or firmware (as the case may be);

(b) take reasonable steps to ensure that the cause of the vulnerability or likely cause of the material adverse effect is rectified, or its potential impact is mitigated, as soon as is reasonably practicable; and

(c) ensure that the Security Sub-Committee is promptly notified of the steps being taken to rectify the cause of the vulnerability or likely cause of the material adverse effect, or to mitigate its potential impact (as the case may be), and the time within which those steps are intended to be completed.

G3.19 A User shall not be required to notify a manufacturer or developer in accordance with

Section G3.18(a) where it has reason to be satisfied that the manufacturer or developer is already aware of the matter that would otherwise be notified.

G3.20 Each User shall, wherever it is practicable to do so, establish with:

(a) the manufacturers of the hardware and developers of the software and firmware which form part of its User Systems; and

(b) (where applicable) any Smart Metering System (excluding a Communications Hub Function or Gas Proxy Function which forms part of a SMETS2+ Device) for which it is the Responsible Supplier,

arrangements designed to ensure that the User will be notified where any such manufacturer or developer (as the case may be) becomes aware of any material security vulnerability in, or likely cause of a material adverse effect on the security of, such hardware, software, firmware or Device.

G3.21 Any arrangements established in accordance with Section G3.20 may provide that the manufacturer or developer (as the case may be) need not be required to notify the User where that manufacturer or developer has reason to be satisfied that the User is already aware of the matter that would otherwise be notified under the arrangements.

G3.21A Where a Manufacturer Party becomes aware of any material security vulnerability in, or likely cause of a material adverse effect on the security of any Device Model in respect of which it is the Manufacturer, it shall comply with the requirements of Section G3.18(b) and (c).

Cryptographic Processing

G3.22 Each User shall ensure that it carries out Cryptographic Processing only within Cryptographic Modules established in accordance with its Information Classification Scheme.

User Systems: Physical Location

G3.23 Each User which is an Eligible User in relation to any Supply Sensitive Service Request shall ensure that:

(a) any Cryptographic Module which constitutes a component of its User Systems

and in which:

(i) any Private Key that is used to Digitally Sign Pre-Commands is held;

(ii) Pre-Commands are Digitally Signed; and

(iii) any SMETS1 Service Request that constitutes a Critical Service Request is Digitally Signed; and

(b) any functionality of its User Systems which is used to apply Supply Sensitive Checks,

is located, operated, configured, tested and maintained in the United Kingdom by User Personnel who are located in the United Kingdom.

G3.24 Each User to which Section G3.23 applies shall ensure that the components and the functionality of its User Systems to which that Section refers are operated from a sufficiently secure environment in accordance with the provisions of Section G5.17.

Supply Sensitive Check

G3.25 Each User which is an Eligible User in relation to any Supply Sensitive Service Request shall ensure that:

(a) it applies a Supply Sensitive Check prior to Digitally Signing a Pre-Command or SMETS1 Service Request in respect of any Supply Sensitive Service Request;

(b) it both applies that Supply Sensitive Check and Digitally Signs the relevant Pre-Command or SMETS1 Service Request in the United Kingdom; and

(c) the relevant Pre-Command or SMETS1 Service Request has been processed only in the United Kingdom between the application of the Supply Sensitive Check and the Digital Signature.

SMETS1 Smart Metering Systems

G3.26 Each Supplier Party shall use its best endeavours to ensure that each SMETS1 SMS for which it is the Responsible Supplier is at all times Secure.

G3.27 Each Supplier Party shall retain documentary evidence sufficient to demonstrate its compliance with the obligation at Section G3.26.

G3.28 For the purposes of Section G3.26:

(a) a SMETS1 SMS is "**Secure**" if it is designed, installed, operated and supported so as to ensure, to an Appropriate Standard, that it is not subject to any event which results, or is capable of resulting, in any Device of which it is comprised being Compromised to a material extent; and

(b) an "**Appropriate Standard**" means a high level of security that is in accordance with good industry practice within the energy industry in Great Britain, and is capable of verification as such by the User Independent Security Assurance Service Provider in accordance with Section G8.

User Use of Private Keys

G3.29 Each User shall ensure that any Private Key that it uses or intends to use to create a Digital Signature that forms part of a Command that is to be sent to a SMETS2+ Device is used only for the purposes of:

(a) creating Digital Signatures that form part of Commands that are to be sent to SMETS2+ Devices; or

(b) Digitally Signing Certificate Signing Requests.

G7 SECURITY SUB-COMMITTEE

Establishment of the Security Sub-Committee

G7.1 The Panel shall establish a Sub-Committee in accordance with the requirements of this Section G7, to be known as the "**Security Sub-Committee**".

G7.2 Save as expressly set out in this Section G7, the Security Sub-Committee shall be subject to the provisions concerning Sub-Committees set out in Section C6 (Sub-Committees).

Membership of the Security Sub-Committee

G7.3 The Security Sub-Committee shall be composed of the following persons (each a "**Security Sub-Committee Member**"):

(a) the Security Sub-Committee Chair (as further described in Section G7.5);

(b) eight Security Sub-Committee (Supplier) Members (as further described in Section G7.6);

(c) two Security Sub-Committee (Network) Members (as further described in Section G7.8);

(d) one Security Sub-Committee (Other User) Member (as further described in Section G7.10);

(e) one Security Sub-Committee (Shared Resource Provider) Member (as further described in Section G7.12);

(c) one Security Sub-Committee (Manufacturer Party) Member as further described in Section G7.13A;

(d) ~~(f)~~ one representative of the DCC (as further described in Section G7.15).

G7.4 Each Security Sub-Committee Member must be an individual (and cannot be a body corporate, association or partnership). No one person can hold more than one office as a Security Sub-Committee Member at the same time.

G7.5 The "**Security Sub-Committee Chair**" shall be such person as is (from time to time) appointed to that role by the Panel in accordance with a process designed to ensure that:

(a) the candidate selected is sufficiently independent of any particular Party or class of Parties;

(b) the Security Sub-Committee Chair is appointed for a three-year term (following which he or she can apply to be re-appointed);

(c) the Security Sub-Committee Chair is remunerated at a reasonable rate;

(d) the Security Sub-Committee Chair's appointment is subject to Section C6.9 (Member Confirmation), and to terms equivalent to Section C4.6 (Removal of Elected Members);

(e) provision is made for the Security Sub-Committee Chair to continue in office for a reasonable period following the end of his or her term of office in the event of any delay in appointing his or her successor; and

(f) where the Security Sub-Committee Chair's appointment (and for the purposes of this Section and Section G7.5A all references to appointment shall encompass re-appointment) is to take effect on or after the date this Section G7.5(f) comes into force, the Panel shall:

(i) notify the Secretary of State of the appointment it proposes to make;

(ii) not make the appointment unless and until the Secretary of State has confirmed in writing that they do not object to the appointment being made;

(iii) ensure that the terms of the appointment include terms which provide for the Panel to terminate the appointment where directed to do so by the Secretary of State pursuant to Section G7.5A and from such date or within such period as may be specified in the Secretary of State's direction; and

(iv) where the appointed person has not, at the date of the appointment, passed (as a minimum) a Security Check (or equivalent), ensure that the

terms of the appointment include terms which:

(A) require the appointed person to apply for a Security Check (or equivalent) within one month of the date of the appointment;

(B) provide for the Panel to terminate the appointment if a Security Check (or equivalent) is not passed by the appointed person within 12 months of the date of the appointment (or such longer period as the Secretary of State may approve following a request from the Panel).

G7.5A The Secretary of State may, in respect of any Security Sub-Committee Chair appointment which takes effect on or after the date Section G7.5(f) comes into force, direct the Panel to terminate the appointment of the Security Sub-Committee Chair where the Secretary of State considers it necessary to do for the purposes of preserving the integrity of, and in the interests of maintaining, the security of the End-to-End Smart Metering System (or any part of that system).

G7.5B The Panel shall comply with any direction given to it by the Secretary of State pursuant to Section G7.5A.

G7.6 Each of the eight "**Security Sub-Committee (Supplier) Members**" shall (subject to any directions to the contrary made by the Secretary of State for the purpose of transition on the incorporation of this Section G7 into this Code):

(a) be appointed in accordance with Section G7.7, subject to compliance by the appointed person with Section C6.9 (Member Confirmation);

(b) retire two years after his or her appointment (without prejudice to his or her ability to be nominated for a further term of office); and

(c) be capable of being removed from office in accordance with Sections C4.5 and C4.6 (Removal of Elected Members), for which purpose those Sections shall be read as if references to "Elected Member" were to "Security Sub-Committee (Supplier) Member", references to "Panel" were to "Security Sub-Committee", references to "Panel Chair" were to "Security Sub-Committee Chair", and references to "Panel Members" were to "Security Sub-Committee

Members".

G7.7 Each of the eight Security Sub-Committee (Supplier) Members shall (subject to Section G7.14) be appointed in accordance with a process:

(a) by which six Security Sub-Committee (Supplier) Members will be elected by Large Supplier Parties, and two Security Sub-Committee (Supplier) Members will be elected by Small Supplier Parties; and

(b) that is otherwise the same as that by which Elected Members are elected under Sections C4.2 and C4.3 (as if references therein to "Panel" were to "Security Sub-Committee", references to "Panel Chair" were to "Security Sub-Committee Chair", references to "Panel Members" were to "Security Sub-Committee Members", and references to provisions of Section C or D were to the corresponding provisions set out in or applied pursuant to this Section G7).

G7.8 Each of the two "**Security Sub-Committee (Network) Members**" shall (subject to any directions to the contrary made by the Secretary of State for the purpose of transition on the incorporation of this Section G7 into this Code):

(a) be appointed in accordance with Section G7.9, subject to compliance by the appointed person with Section C6.9 (Member Confirmation);

(b) retire two years after his or her appointment (without prejudice to his or her ability to be nominated for a further term of office); and

(c) be capable of being removed from office in accordance with Sections C4.5 and C4.6 (Removal of Elected Members), for which purpose those Sections shall be read as if references to "Elected Member" were to "Security Sub-Committee (Network) Member", references to "Panel" were to "Security Sub-Committee", references to "Panel Chair" were to "Security Sub-Committee Chair", and references to "Panel Members" were to "Security Sub-Committee Members".

G7.9 Each of the two Security Sub-Committee (Network) Members shall (subject to Section G7.14) be appointed in accordance with a process:

(a) by which one Security Sub-Committee (Network) Member will be elected by the Electricity Network Parties and one Security Sub-Committee (Network) Member will be elected by the Gas Network Parties; and

(b) that is otherwise the same as that by which Elected Members are elected under Sections C4.2 and C4.3 (as if references therein to "Panel" were to "Security Sub-Committee", references to "Panel Chair" were to "Security Sub-Committee Chair", references to "Panel Members" were to "Security Sub-Committee Members", and references to provisions of Section C or D were to the corresponding provisions set out in or applied pursuant to this Section G7).

G7.10 The "**Security Sub-Committee (Other User) Member**" shall (subject to any directions to the contrary made by the Secretary of State for the purpose of transition on the incorporation of this Section G7 into this Code):

(a) be appointed in accordance with Section G7.11, subject to compliance by the appointed person with Section C6.9 (Member Confirmation);

(b) retire two years after his or her appointment (without prejudice to his or her ability to be nominated for a further term of office); and

(c) be capable of being removed from office in accordance with Sections C4.5 and C4.6 (Removal of Elected Members), for which purpose those Sections shall be read as if references to "Elected Member" were to "Security Sub-Committee (Other User) Member", references to "Panel" were to "Security Sub-Committee", references to "Panel Chair" were to "Security Sub-Committee Chair", and references to "Panel Members" were to "Security Sub-Committee Members".

G7.11 The Security Sub-Committee (Other User) Member shall (subject to Section G7.14) be appointed in accordance with a process:

(a) by which he or she is elected by those Other SEC Parties which are Other Users; and

(b) that is otherwise the same as that by which Elected Members are elected under Sections C4.2 and C4.3 (as if references therein to "Panel" were to "Security

Sub-Committee", references to "Panel Chair" were to "Security Sub-Committee Chair", references to "Panel Members" were to "Security Sub-Committee Members", and references to provisions of Section C or D were to the corresponding provisions set out in or applied pursuant to this Section G7).

G7.12 The "**Security Sub-Committee (Shared Resource Provider) Member**" shall:

(a) be appointed in accordance with Section G7.13, subject to compliance by the appointed person with Section C6.9 (Member Confirmation);

(b) retire two years after his or her appointment (without prejudice to his or her ability to be nominated for a further term of office); and

(c) be capable of being removed from office in accordance with Sections C4.5 and C4.6 (Removal of Elected Members), for which purpose those Sections shall be read as if references to "Elected Member" were to "Security Sub-Committee (Shared Resource Provider) Member", references to "Panel" were to "Security Sub-Committee", references to "Panel Chair" were to "Security Sub-Committee Chair", and references to "Panel Members" were to "Security Sub-Committee Members".

G7.13 The Security Sub-Committee (Shared Resource Provider) Member shall (subject to Section G7.14) be appointed in accordance with a process:

(a) by which he or she is elected by those Other SEC Parties which are Shared Resource Providers; and

(b) that is otherwise the same as that by which Elected Members are elected under Sections C4.2 and C4.3 (as if references therein to "Panel" were to "Security Sub-Committee", references to "Panel Chair" were to "Security Sub-Committee Chair", references to "Panel Members" were to "Security Sub-Committee Members", and references to provisions of Section C or D were to the corresponding provisions set out in or applied pursuant to this Section G7).

G7.13A The "**Security Sub-Committee (Manufacturer Party) Member**" shall:

(a) be appointed in accordance with Section G7.13B, subject to compliance by the

appointed person with Section C6.9 (Member Confirmation);

(b) retire two years after his or her appointment (without prejudice to his or her ability to be nominated for a further term of office); and

(c) be capable of being removed from office in accordance with Sections C4.5 and C4.6 (Removal of Elected Members), for which purpose those Sections shall be read as if references to "Elected Member" were to "Security Sub-Committee (Manufacturer Party) Member", references to "Panel" were to "Security Sub-Committee", references to "Panel Chair" were to "Security Sub-Committee Chair", and references to "Panel Members" were to "Security Sub-Committee Members".

G7.13B The Security Sub-Committee (Manufacturer Party) Member shall (subject to Section G7.14) be appointed in accordance with a process:

(a) by which he or she is elected by those Other SEC Parties which are Manufacturer Parties; and

(b) that is otherwise the same as that by which Elected Members are elected under Sections C4.2 and C4.3 (as if references therein to "Panel" were to "Security Sub-Committee", references to "Panel Chair" were to "Security Sub-Committee Chair", references to "Panel Members" were to "Security Sub-Committee Members", and references to provisions of Section C or D were to the corresponding provisions set out in or applied pursuant to this Section G7).

G7.14 The following shall apply in respect of all candidates nominated or re-nominated for election as a Security Sub-Committee (Supplier) Member, Security Sub-Committee (Network) Member, Security Sub-Committee (Other User) Member ~~or~~, Security Sub-Committee (Shared Resource Provider) Member or Security Sub-Committee (Manufacturer Party) Member:

(a) the Security Sub-Committee may, by no later than 5 Working Days following the expiry of the period of time set out in the request for nominations, reject a candidate (by notifying the candidate of such rejection) where the Security Sub-Committee determines that the candidate does not satisfy one or more of the

following requirements:

(i) the candidate must have been nominated by a company or other organisation, and the individual who submitted the nomination on behalf of the organisation must hold a senior position within the organisation;

(ii) the organisation which nominated the candidate must have confirmed that it is satisfied that the candidate has the relevant security expertise in relation to the category of membership of the Security Sub-Committee for which the candidate has been nominated;

(iii) the organisation which nominated the candidate must have confirmed that the candidate has successfully completed a BS7858 security assessment (or a security assessment named by such organisation which the organisation confirms to be equivalent); and

(iv) the candidate must have sufficient security expertise in relation to the category of membership of the Security Sub-Committee for which the candidate has been nominated;

(b) a candidate who is rejected under paragraph (a) above shall not (subject to paragraph (c) below) be an eligible candidate for the relevant election;

(c) where a candidate disputes a rejection notification under paragraph (a) above, the candidate shall have 3 Working Days following receipt of such notification to refer the matter to the Panel for its final determination of whether the candidate satisfies the requirements set out in paragraph (a) above; and

(d) where necessary, the Secretariat shall delay giving notice of the names of eligible candidates pending expiry of the time periods set out in paragraph (a) and/or (c) or determination by the Panel under paragraph (c) (as applicable).

G7.15 The DCC may nominate one person to be a Security Sub-Committee Member by notice to the Secretariat from time to time. The DCC may replace its nominee from time to time by prior notice to the Secretariat. Such nomination or replacement shall be subject to compliance by the relevant person with Section C6.9 (Member Confirmation).

Proceedings of the Security-Sub Committee

G7.16 Without prejudice to the generality of Section C5.13(c) (Attendance by Other Persons) as it applies pursuant to Section G7.17:

(a) a representative of the Secretary of State and a representative of the Authority shall be:

(i) invited to attend each and every Security Sub-Committee meeting;

(ii) entitled to speak at such Security Sub-Committee meetings without the permission of the Security Sub-Committee Chair; and

(iii) provided with copies of all the agenda and supporting papers available to Security Sub-Committee Members in respect of such meetings;

(b) the Security Sub-Committee Chair shall invite to attend Security Sub-Committee meetings any persons that the Security Sub-Committee determines it appropriate to invite in order to be provided with expert advice on security matters.

G7.17 Subject to Section G7.16, the provisions of Section C5 (Proceedings of the Panel) shall apply to the proceedings of the Security Sub-Committee, for which purpose that Section shall be read as if references to "Panel" were to "Security Sub-Committee", references to "Panel Chair" were to "Security Sub-Committee Chair", and references to "Panel Members" were to "Security Sub-Committee Members".

Duties and Powers of the Security Sub-Committee

G7.18 The Security Sub-Committee:

(a) shall perform the duties and may exercise the powers set out in Sections G7.19 to G7.23; and

(b) shall perform such other duties and may exercise such other powers as may be expressly ascribed to the Security Sub-Committee elsewhere in this Code.

<u>Document Development and Maintenance</u>

G7.19 The Security Sub-Committee shall:

(a) develop and maintain documents, to be known as the "**Security Controls Framework**", which shall set out the appropriate User and DCC Security Assessment Methodology to be applied to different categories of security assurance assessment carried out in accordance with Section G8 (User Security Assurance) and Section G9 (DCC Security Assurance) and be designed to ensure that such security assurance assessments are proportionate; and

(i) achieve appropriate levels of security assurance in respect of different Users and different User Roles, and the DCC; and

(ii) in the case of User related assessments are consistent in their treatment of equivalent Users and equivalent User Roles, and;

(b) carry out reviews of the Security Risk Assessment:

(i) at least once each year in order to identify any new or changed security risks to the End-to-End Smart Metering System; and

(ii) in any event promptly if the Security Sub-Committee considers there to be any material change in the level of security risk;

(c) maintain the Security Requirements to ensure that it is up to date and at all times identifies the security controls which the Security Sub-Committee considers appropriate to mitigate the security risks identified in the Security Risk Assessment;

(d) maintain the End-to-End Security Architecture to ensure that it is up to date;

(e) develop and maintain a document to be known as the "**Risk Treatment Plan**", which shall identify the residual security risks which in the opinion of the Security Sub-Committee remain unmitigated taking into account the security controls that are in place;

(e) with respect to the CPA Security Characteristics:

(i) ~~(f) liaise and work with the NCSC to develop and~~ maintain CPA Security

Characteristics that set out the levels of security required for Smart Meters, Communications Hubs, SAPCs and HCALCs; and

(ii) where it considers it appropriate from time to time, develop the CPA Security Characteristics so as additionally to set out levels of security required for any other Device,

in each case so as to ensure that the required levels of security are proportionate and appropriate taking into consideration the security risks identified in the Security Risk Assessment; ~~and~~

(f) develop and maintain a document to be known as the **"CPA Policies and Procedures"** which shall:

(i) set out the steps that a Manufacturer must follow in order to obtain and maintain a CPA Certificate in respect of a Device Model;

(ii) set out the criteria that a Test Lab must satisfy in order to perform the functions of a CPA Test Lab for the purposes of the CPA Scheme;

(iii) describe the procedures that a CPA Test Lab must apply in evaluating whether a Device Model should be issued with a CPA Certificate;

(iv) make such other provision in relation to the evaluation and assessment of a Device Model for the purposes of the CPA Scheme as the Security Sub-Committee may consider appropriate;

(v) make such provision relating to the expiry, renewal, suspension, withdrawal and cancellation of CPA Certificates as the Security Sub-Committee may consider appropriate; and

(vi) make such provision in relation to the role of the CPA Scheme Operator as the Security Sub-Committee may consider appropriate;

(g) develop and maintain documents to be known as the **"CPA Assurance Maintenance Plan"** which shall describe the components of a Device that, if changed, will require a new CPA Certificate to be issued; and

(h) ~~(g)~~ develop and maintain ~~documents~~a document to be known as the **"SSC Guidance for Device Security Assurance and Triage"** which shall set out the ~~SSC's~~ guidance ~~on~~of the Security Sub-Committee in respect of the requirements and processes which are to be followed in respect of Devices (including in relation to their ~~triage~~Triage and refurbishment) in order to:

(i) achieve appropriate levels of security assurance in accordance with the requirement of this Code; and

(ii) obtain and maintain a CPA ~~Certification~~Certificate.

Security Assurance

G7.20 The Security Sub-Committee shall:

(a) periodically, and in any event at least once each year, review the Security Obligations and Assurance Arrangements in order to identify whether in the opinion of the Security Sub-Committee they continue to be fit for purpose;

(b) exercise such functions as are allocated to it under, and comply with the applicable requirements of Section G8 (User Security Assurance) and Section G9 (DCC Security Assurance);

(c) provide the Panel with support and advice in respect of issues relating to the actual or potential non-compliance of any Party with the requirements of the Security Obligations and Assurance Arrangements;

(d) ~~keep under review the NCSC CPA Certificate scheme in order to assess whether it continues to be fit for purpose in so far as it is relevant to the Code, and suggest modifications to the scheme provider to the extent to which it considers them appropriate;~~exercise such functions as are allocated to it under, and comply with the applicable requirements of, Section G13 (CPA Scheme Operator) with the objective of ensuring that there are available at all times CPA Scheme Operator Services which are both suitable in nature and sufficient in quantity to meet the reasonable requirements of the CPA Scheme;

(e) to the extent to which it considers it appropriate, in relation to any User (or,

during the first User Entry Process, Party) which has produced a User Security Assessment Response that sets out any steps that the User proposes to take in accordance with Section G8.24(b):

(i) liaise with that User (or Party) as to the nature and timetable of such steps;

(ii) either accept the proposal to take those steps within that timetable or seek to agree with that User (or Party) such alternative steps or timetable as the Security Sub-Committee may consider appropriate; and

(iii) take advice from the User Independent Security Assurance Service Provider; and

(iv) where the Security Sub-Committee considers it appropriate, request the User Independent Security Assurance Service Provider to carry out a Follow-up Security Assessment;

(f) provide advice to the Panel on the scope and output of the independent security assurance arrangements of the DCC in relation to the design, building and testing of the DCC Total System;

(g) to the extent to which it considers appropriate , in relation to the DCC which has produced a DCC Security Assessment Response that sets out any steps that the DCC proposes to take in accordance with Section G9.24(b):

(i) liaise with the DCC as to the nature and timetable of such steps;

(ii) either accept the proposal to take those steps within that timetable or seek to agree with the DCC such alternative steps or timetable as the Security Sub-Committee may consider appropriate;

(iii) take advice from the DCC Independent Security Assessment Service Provider; and

(iv) where the Security Sub-Committee considers it appropriate, request the DCC Independent Security Assessment Service Provider to carry out a Follow-up Security Assessment;

(h) provide advice to the:

(i) Panel in relation to the appointment of the User Independent Security Assurance Service Provider, monitor the performance of the person appointed to that role and provide advice to the Panel in respect of its views as to that performance; and

(ii) DCC in relation to the appointment of the DCC Independent Security Assessment Service Provider, monitor the performance of the person appointed to that role and provide advice to the DCC in respect of its views as to that performance;

(i) provide advice and information to the Authority in relation to any actual or potential non-compliance with the CPA Security Characteristics of any Device or apparatus in respect of which a CPA Certificate is issued or required.

Monitoring and Advice

G7.21 The Security Sub-Committee shall:

(a) provide such reasonable assistance to the DCC and Users as may be requested by them in relation to the causes of security incidents and the management of vulnerabilities on their Systems;

(b) monitor the (actual and proposed) Anomaly Detection Thresholds of which it is notified by the DCC, consider the extent to which they act as an effective means of detecting any Compromise to any relevant part of the DCC Total System or of any User Systems, and provide its opinion on such matters to the DCC;

(c) provide the Panel with support and advice in respect of Disputes for which the Panel is required to make a determination, insofar as such Disputes relate to the Security Obligations and Assurance Arrangements;

(d) provide the Panel, the Change Sub-Committee, the Change Board and any relevant Working Group with support and advice in relation to any Draft Proposal or Modification Proposal which may affect the security of the End-

to-End Smart Metering System or the effective implementation of the security controls that are identified in the Security Requirements;

(e) advise the Authority of any modifications to the conditions of Energy Licences which it considers may be appropriate having regard to the residual security risks identified from time to time in the Risk Treatment Plan;

(f) respond to any consultations on matters which may affect the security of the End-to-End Smart Metering System or the effective implementation of the security controls that are identified in the Security Requirements;

(g) act in cooperation with, and send a representative to, the SMKI PMA, the Technical Architecture and Business Architecture Sub-Committee and any other Sub-Committee or Working Group which requests the support or attendance of the Security Sub-Committee;

(h) (to the extent to which it reasonably considers that it is necessary to do so) liaise and exchange information with, provide advice to, and seek the advice of the At HAN Forum on matters relating to the Alt HAN Arrangements which may affect the security of the End-to-End Smart Metering System or the effective implementation of the security controls that are identified in the Security Requirements;

(i) provide such further support and advice to the Panel as it may request; and

(j) provide the Authority with such information and documents as it may reasonably request in relation to any matter referred by a Party to the Authority for determination pursuant to Section F2.7B.

Modifications

G7.22 The Security Sub-Committee shall establish a process under which the Code Administrator monitors Draft Proposals and Modification Proposals with a view to identifying (and bringing to the attention of the Security Sub-Committee) those proposals that:

(a) are likely to affect the Security Obligations and Assurance Arrangements; or

(b) are likely to relate to other parts of the Code but may have a material effect on the security of the End-to-End Smart Metering System,

and the Code Administrator shall comply with such process.

G7.23 Notwithstanding Section D1.3 (Persons Entitled to Submit Draft Proposals):

(a) the Security Sub-Committee shall be entitled to submit Draft Proposals in respect of the Security Obligations and Assurance Arrangements where the Security Sub-Committee considers it appropriate to do so; and

(b) any Security Sub-Committee Member shall be entitled to submit Draft Proposals in respect of the Security Obligations and Assurance Arrangements where he or she considers it appropriate to do so (where the Security Sub-Committee has voted not to do so).

G7.24 Notwithstanding and subject to the provisions of the Working Group Terms of Reference, the Security Sub-Committee shall be entitled to nominate a representative to be a member of any Working Group.

G7.25 For the purposes of Section D7.1 (Modification Report):

(a) written representations in relation to the purpose and effect of a Modification Proposal may be made by:

(i) the Security Sub-Committee; and/or

(ii) any Security Sub-Committee Member (either alone or in addition to any representations made by other Security Sub-Committee Members and/or the Security Sub-Committee collectively); and

(b) notwithstanding Section D7.3 (Content of the Modification Report), the Code Administrator shall ensure that all such representations, and a summary of any evidence provided in support of them, are set out in the Modification Report prepared in respect of the relevant Modification Proposal.

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,

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; and

(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);

(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) one or more of the requirements specified in Section G8.5; and

(b) the requirement 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 a CTAS provider;

(b) 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

(c) holds another membership, accreditation, approval or form of professional validation that is in the opinion of the Panel substantially equivalent in status and effect to one or more of the arrangements described in paragraphs (a) and (b).

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

(a) employs consultants who are members of the Certified Cyber Professional (CCP) and the Certified Cyber Security Consultancy (CCSC) schemes at the 'Lead' or 'Senior Practitioner' level 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 taking 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 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

(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.

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 Sections 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 Section G5 (Information Security: Obligations on the DCC);

(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) one or more of 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 one or more of the arrangements described in paragraphs (a) and (b).

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

(a) employs consultants who are certified under the Certified Cyber Security Consultancy (CCSC) scheme and have experience of operating at the 'Lead' or 'Senior Practitioner' level 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~~G9.

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

(b) addresses the findings set out in the report; and

(c) 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 noncompliance 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.

G13 The CPA Scheme Operator

Procurement of the CPA Scheme Operator

G13.1 The Security Sub-Committee shall procure the provision of services in relation to the operation of the CPA Scheme:

(a) of the scope specified in Section G13.3;

(b) from a person who:

(i) is suitably qualified in accordance with Section G13.4; and

(ii) is suitably independent in accordance with Section G13.5,

and that person is referred to in this Section G13 as the "**CPA Scheme Operator**".

G13.2 The Security Sub-Committee may appoint more than one person to carry out the functions of the CPA Scheme Operator.

Scope of CPA Scheme Operator Services

G13.3 The services specified in this Section G13.3 (the "**CPA Scheme Operator Services**") are services in accordance with which the CPA Scheme Operator shall:

(a) develop a standard form of contract (which shall require to be approved by the Security Sub-Committee) to be entered into by Manufacturers seeking to obtain a CPA Certificate in relation to a Device Model;

(b) develop a standard form of contract (which shall require to be approved by the Security Sub-Committee, and following such approval shall be known as the "**CPA Test Lab Framework Agreement**") to be entered into by CPA Test Labs in relation to the performance of their functions for the purposes of the CPA Scheme;

(c) enter into the contracts developed under paragraphs (a) and (b) with relevant Manufacturers and CPA Test Labs;

(d) issue CPA Certificates to Manufacturers in relation to Device Models which

have been successfully demonstrated to satisfy the requirements of the CPA Security Characteristics;

(e) renew, suspend, withdraw and cancel CPA Certificates in such circumstances as may from time to time be described in the CPA Policies and Procedures;

(f) carry out such evaluation (and related) functions as may from time to time be set out in the CPA Policies and Procedures, or which it is otherwise requested by the Security Sub-Committee to carry out, which may include in particular:

(i) assessing, and from time to time reviewing, whether a Test Lab which wishes to perform the functions of a CPA Test Lab meets the criteria specified for that purpose in the CPA Policies and Procedures;

(ii) where a Test Lab does not meet the criteria specified in the CPA Policies and Procedures for performing the functions of a CPA Test Lab, advising on the reasons for the failure and the changes or additional evidence that would be needed in order for it to meet those criteria;

(iii) responding to technical enquiries from Manufacturers and CPA Test Labs in relation to the evaluation process for Device Models in respect of which a CPA Certificate is being (or is proposed to be) sought (the "**evaluation process**");

(iv) reviewing and approving the proposed testing regime in respect of any Device Model for which a CPA Certificate is being sought;

(v) reviewing the results of tests carried out by a CPA Test Lab in relation to a Device Model for which a CPA Certificate is being sought, in order to:

(A) determine whether a CPA Certificate should be issued in respect of that Device Model; and

(B) where a Device Model has not satisfied the requirements for the issue of a CPA Certificate, advising on the reasons for the failure and the changes or additional evidence that would be needed in

order to it to be issued with a CPA Certificate;

(vi) liaising with, and providing information and support to, CPA Test Labs and Manufacturers in relation to the evaluation process; and

(vii) providing such information and advice to the Security Sub-Committee as may be requested from time to time;

(g) overseeing the interactions between Manufacturers and CPA Test Labs in relation to the evaluation process;

(h) providing information, advice and support to any Test Labs which wishes to perform the functions of a CPA Test Lab for the purposes of the CPA Scheme;

(i) attending meetings of the Security Sub-Committee whenever requested to do so by the Security Sub-Committee Chair for the purpose of providing advice and information, and otherwise delivering such reports or presentations, as may be requested;

(j) providing such written reports, advice and information to the Security Sub-Committee, in relation to the operation of the CPA Scheme and the provision of the CPA Scheme Operator Services, as it may from time to time request;

(k) providing such other support and assistance to the Security Sub-Committee as it may from time to time request; and

(l) undertake such other activities, and do so at such times and in such manner, as may be further provided for in this Section G13.

Suitably Qualified Person

G13.4 The CPA Scheme Operator shall be treated as suitably qualified in accordance with this Section G13.4 only if it satisfies such requirements as to its qualifications as the Security Sub-Committee may from time to time determine for the purposes of the process of procuring services in relation to the operation of the CPA Scheme.

Independence Requirement

G13.5 The CPA Scheme Operator shall be treated as suitably independent in accordance with this Section G13.5 only if it satisfies

(a) the requirements specified in Section G13.7; and

(b) the requirements specified in Section G13.8.

G13.6 For the purposes of Sections G13.7 and G13.8:

(a) a "**Relevant Person**" means any of the following:

(i) the DCC;

(ii) a DCC User;

(iii) the owner or operator of any Test Lab which performs the functions of a CPA Test Lab for the purposes of the CPA Scheme;

(iv) the Manufacturer of any Device which requires a CPA Certificate;

(b) a "**Relevant Service Provider**" means any service provider to a Relevant Person from which that Relevant Person acquires capability for a purpose related to the CPA Scheme.

G13.7 The requirements specified in this Section G13.7 are that:

(a) no Relevant Person 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 CPA Scheme Operator;

(b) no director of any Relevant Person, 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 CPA Scheme Operator; and

(c) the CPA Scheme Operator does not hold or acquire a participating interest (as defined in section 421A of the Financial Services and Markets Act 2000) in any Relevant Person or any Relevant Service Provider,

(but for these purposes references to a Relevant Service Provider shall not include the CPA Scheme Operator where it acts in that capacity).

G13.8 The requirements specified in this Section G13.8 are that the CPA Scheme Operator is able to demonstrate to the satisfaction of the Security Sub-Committee that it:

(a) 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 Person or Relevant Service Provider (and for these purposes a 'commercial relationship' shall include a relationship established by virtue of the CPA Scheme Operator itself being a Relevant Service Provider to any Relevant Person); and

(b) satisfies such other requirements as to its independence as the Security Sub-Committee may from time to time determine for the purposes of the process of procuring services in relation to the operation of the CPA Scheme.

Compliance of the CPA Scheme Operator

G13.9 The Security Sub-Committee shall be responsible for ensuring that the CPA Scheme Operator provides the CPA Scheme Operator Services, and carries out its functions as such, in accordance with the provisions of this Section G13.

G14 The CPA Transition Approach Document

Overview

G14.1 The **CPA Transition Approach Document** is to be developed by the Secretary of State and incorporated into this Code pursuant to Part G of Condition 22 of the DCC Licence and Section X5 (Incorporation of Certain Documents into this Code).

Purpose of the CPA Transition Approach Document

G14.2 The purpose of the CPA Transition Approach Document is to:

(a) provide that the Revised CPA Arrangements shall not have full effect immediately;

(b) enable the gradual implementation of and transition to the Revised CPA Arrangements; and

(c) provide for additional and/or varied provisions to apply for a transitional period to manage the interactions between the Revised CPA Arrangements and the previous arrangements for the CPA Scheme.

Content of the CPA Transition Document

G14.3 The CPA Transition Document may include, without limitation, some or all of the following:

(a) a modification process which enables the Security Sub-Committee to modify the CPA Transition Approach Document;

(b) rights and/or obligations of the DCC and other Parties designed to facilitate or achieve the purposes of the CPA Transition Approach Document which are either additional to or vary other rights and/or obligations set out in this Code;

(c) variations to the powers and/or duties of the Panel, the Security Sub-Committee and/or any other Sub-Committee designed to facilitate or achieve the purposes of the CPA Transition Approach Document which are either additional to or vary other powers and/or duties set out in this Code;

(d) variations to the processes by which CPA Testing is administered, managed and/or operated, which may include variations to the requirements which apply to CPA Test Labs and/or Manufacturers;

(e) mechanisms for completion or in-flight transfer of Device Models that are undergoing testing as part of the arrangements for the CPA Scheme which existed prior to the Revised CPA Arrangements;

(f) pre-conditions that may need to apply prior to some or all of the Revised CPA Arrangements coming into effect;

(g) variations in the arrangements for issuing of CPA Certificates, and/or the addition or removal of Device Models to or from the Certified Products List;

(h) limitations and/or variations to the rights and/or obligations of the Parties to apply for a transitional period prior to the full implementation of the Revised CPA Arrangements;

(i) provision for the referral and determination of disputes in respect of the CPA Transition Approach Document, which may include interim or final determinations by the Secretary of State, the Authority, the Security Sub-Committee, the Panel or any other person specified by the Secretary of State; and

(j) a date from which the CPA Transition Approach Document shall cease to have effect, or a mechanism for determining such date.

Definitions

G14.4 For the purposes of this Section G14:

Revised CPA Arrangements	means the modifications made to this Code, including in particular the addition to this Code of Section G13 (The CPA Scheme Operator), in order to incorporate into this Code provisions for

	the administration and governance of the CPA Scheme.

Section L

IKI Certificates

L3.20 Where SECCo or any Party ~~or Manufacturer~~ or RDP is an Authorised Subscriber in accordance with the IKI Certificate Policy, it will be an Eligible Subscriber in respect of an IKI Certificate in the circumstances set out in the IKI Certificate Policy.

Appendix Q

1.3.3 Subscribers

(A) In accordance with Section L3.20 of the Code (IKI Certificates), certain Parties, ~~Manufacturers,~~ RDPs and SECCo may become Authorised Subscribers.

1.4.2 Prohibited Certificate Uses

(i) No Party, ~~Manufacturer,~~ RDP or SECCo shall use a Certificate other than for the purposes specified in Part 1.4.1 of this Policy.

3.2.2 Authentication of Organisation Identity

(A) Provision is made in the SMKI RAPP section 5.5 in relation to the:

(i) procedure to be followed by a Party, ~~Manufacturer,~~ RDP or SECCo in order to become an Authorised Subscriber;

(ii) criteria in accordance with which the ICA will determine whether a Party, ~~Manufacturer,~~ RDP or SECCo is entitled to become an Authorised Subscriber; and

(iii) requirement that the Party, ~~Manufacturer,~~ RDP or SECCo shall be Authenticated by the ICA for that purpose.

(B) Provision is made in the SMKI RAPP section 5 for the purpose of ensuring that the criteria in accordance with which the ICA shall Authenticate a Party, ~~Manufacturer,~~

RDP or SECCo shall be set to the level pursuant to the SMKI PMA Guidance on 'Verifying Organisation Identity' published on the Website.

4.2.2 Approval or Rejection of Certificate Applications

(A) Where any Certificate Signing Request fails to satisfy the requirements set out in the SMKI RAPP, this Policy or any other provision of the Code, the ICA:

(i) shall reject it and refuse to Issue the Certificate which was the subject of the Certificate Signing Request; and

(ii) shall give notice to the Party, ~~Manufacturer,~~ RDP or SECCo which made the Certificate Signing Request of the reasons for its rejection.

Annex A: Definitions and Interpretation

Authorised Responsible Officer (ARO)	means an individual that has successfully completed the process for becoming an ARO on behalf of a Party, ~~Manufacturer,~~ an RDP, a DCC Service Provider or SECCo in accordance with the SMKI RAPP.
Authorised Subscriber	means a Party, ~~Manufacturer,~~ RDP or SECCo which has successfully completed the procedures set out in this Policy and has been authorised by the ICA to submit a Certificate Signing Request.
Eligible Subscriber	means an Authorised Subscriber and: a) in respect of each IKI Certificate Issued by the IKI Administrator CA or the IKI Registration Authority CA, the DCC; b) in respect of each IKI Certificate Issued by the IKI Authorised Organisation Subscriber CA,

	each Eligible Subscriber in respect of Organisation Certificates; c) in respect of each IKI Certificate Issued by the IKI Authorised Device Subscriber CA, each Eligible Subscriber in respect of Device Certificates; d) in respect of each IKI Certificate Issued by the IKI Authorised Web Service Subscriber CA, each Eligible Subscriber for Device Certificates that is the DCC or a Supplier; ~~or~~ e) in respect of each ICA Certificate, the DCC; or f) in respect of each IKI Certificate Issued by the IKI File Signing Certification Authority, an Authorised Subscriber that is a Party, ~~Manufacturer,~~ RDP or SECCo.
Subscriber	means, in relation to any Certificate, a Party, ~~Manufacturer,~~ RDP or SECCo which has been Issued with and accepted that Certificate, acting in its capacity as the holder of the Certificate.

3. SMKI Roles

This SMKI RAPP details the roles of Parties, RDPs, ~~Manufacturers,~~ SECCo and the DCC in the context of access to SMKI Services and/or the SMKI Repository Service as set out in the Code, this SMKI RAPP and the SMKI interface documents. The SMKI RAPP sets out the procedures by which nominated individuals may become Senior Responsible Officers and/or Authorised Responsible Officers in order to act on behalf of a Party, RDP, ~~Manufacturer,~~ SECCo or the DCC (acting in its role as DCC Service Provider) in respect of SMKI Services and the SMKI Repository Service.

This SMKI RAPP also details the obligations in respect of the SMKI Registration Authority and the individuals acting on its behalf as SMKI Registration Authority Managers or SMKI Registration Authority Personnel.

From time to time, the SMKI PMA may require documents or information to be lodged in the SMKI Repository. In such instances, it shall submit a request via the Service Desk and provide such documents and/or information to be lodged in the SMKI Repository. The DCC shall lodge documents and/or information provided to the SMKI Repository, as soon as reasonably practicable following receipt.

3.1 Party, RDP, ~~Manufacturer,~~ SECCo and DCC representatives

Individuals permitted to act as representatives of a Party, RDP, ~~Manufacturer,~~ SECCo or the DCC (in its role as DCC Service Provider) are as set out immediately below:

- Senior Responsible Officer (SRO). The process by which an individual is nominated and their authorisation is checked and their identity verified, so as to be an SRO and act on behalf of an organisation is set out in SMKI RAPP Section 5.2. An individual is nominated to become an SRO by a Director or Company Secretary for a Party, RDP, ~~Manufacturer,~~ SECCo or the DCC (for DCC Service Provider personnel). Once an individual has become an SRO, the SRO may at any time nominate individuals to undertake to become Authorised Responsible Officers (AROs) and to access SMKI Services and/or the SMKI Repository Service. An SRO may also nominate themselves to become an ARO as described below.

- Authorised Responsible Officer (ARO). The process by which an individual is nominated, verified and authorised to be an ARO is set out in SMKI RAPP Section 5.3. The means by which AROs are provided with credentials to authenticate access to SMKI Services and/or the SMKI Repository Service is set out in Section 5.4. The DCC shall permit only AROs to act on behalf of a Party, RDP, ~~Manufacturer,~~ SECCo or the DCC (in its role as DCC Service Provider) for the purposes of accessing SMKI Services and/or the SMKI Repository Service. Depending upon the processes followed, an ARO may also be authorised to act on behalf of a Party, RDP or the DCC (in its role as DCC Service Provider) to be an Authorised Subscriber for Organisation Certificates, Device Certificates or both, following successful completion of SMKI and Repository Entry Process Tests. All AROs are also permitted to access the SMKI Repository Service on behalf of the organisation that they represent, as set out in the SMKI Repository Interface Design Specification.

Each Party, RDP, ~~Manufacturer,~~ SECCo or the DCC (in its role as DCC Service Provider) that wishes to:

a) become an Authorised Subscriber for Organisation Certificates and/or Device Certificates;

b) become an Authorised Subscriber for an IKI Certificate for the purposes of Digitally Signing of files;

or

c) have access only to the SMKI Repository,

shall have at least one ARO successfully appointed (and therefore one SRO).

The DCC shall not be required to repeat processes in relation to an individual for the purposes of verifying their identity for the purposes of becoming an SRO and/or ARO in respect of SMKI Services or the SMKI Repository Service, where the required verification processes have already been carried out for the purposes of identifying them as being a DCCKI SRO and/or DCCKI ARO respectively.

The DCC and any Party or RDP may agree that any action taken by either of them prior to the date of the designation of this SMKI RAPP shall, if the equivalent action taken after that date would have satisfied a requirement of this SMKI RAPP for the purposes of appointing an ARO or SRO or the Party or RDP becoming an Authorised Subscriber, be treated as if it had taken place after that date.

3.2 SMKI Registration Authority representatives

Individuals acting as representatives of the DCC in its role as SMKI Registration Authority are:

- SMKI Registration Authority Manager. The process by which a SMKI Registration Authority Manager is nominated, verified, authorised and provided with the means to authenticate their access to SMKI Services and/or the SMKI Repository Service is set out in SMKI RAPP Sections 6.2 and 6.4.

- SMKI Registration Authority Personnel. The process by which SMKI Registration Authority Personnel are nominated, verified, authorised and provided with the means to authenticate their access to SMKI Services and/or SMKI Repository is set out in SMKI RAPP Sections 6.3 and 6.4.

The DCC shall ensure that only a SMKI Registration Authority Manager or SMKI Registration Authority Personnel may act on behalf of the DCC in respect of matters relating to the SMKI Registration Authority. Each Party, RDP, ~~Manufacturer,~~ SECCo and the DCC (in its role of DCC Service Provider) shall refrain from dealing with DCC Personnel (including SMKI Registration Authority Managers and SMKI Registration Authority Personnel) other than as directed by the Service Desk for the purposes of submitting Certificate Signing Requests (CSRs) and Certificate Revocation Requests (CRRs).

The DCC, in order to perform its role as SMKI Registration Authority, shall nominate at least two individuals to become a SMKI Registration Authority Manager, each of which will have responsibility for:

a) management of the SMKI Registration Authority function and SMKI Registration Authority Personnel;

b) nomination of individuals to become SMKI Registration Authority Personnel;

c) authentication and verification of SMKI Registration Authority Personnel, as set out in Section 6.3 of this document;

d) provision of the means to authenticate access to SMKI Services and/or the SMKI Repository Service for authorised Party, RDP~~, Manufacturer~~ or SECCo representatives and DCC Personnel (including SMKI Registration Authority Personnel);

e) managing the process by which documents and information are lodged in the SMKI Repository; and

f approval of CRRs.

A SMKI Registration Authority Manager may nominate individuals to become SMKI Registration Authority Personnel and to act on behalf of the SMKI Registration Authority as set out in this SMKI RAPP and the Code. The primary responsibilities of SMKI Registration Authority Personnel are:

a) to conduct registration processes as set out in SMKI RAPP Sections 5.1 to 5.5, incorporating:

i. verification of organisational identity;

ii. verification and authorisation of individuals nominated to become SROs or AROs, as set out in Section 5.2 and 5.3 of this document;

iii. provision of the means to authenticate access to SMKI Services and/or the SMKI Repository Service for authorised Party, RDP, ~~Manufacturer,~~ SECCo representatives and DCC personnel; and

iv. assessment of whether an organisation qualifies to become an Authorised Subscriber for Organisation Certificates and/or Device Certificates.

b) processing and approval (where required) of Certification Signing Requests and processing of Certificate Revocation Requests; and

c) processing of requests for revocation of credentials used to access SMKI Services and/or the SMKI Repository Service.

The DCC shall ensure that SMKI Registration Authority Managers and SMKI Registration Authority Personnel, where required, are available to undertake the obligations in respect of procedures set out in this SMKI RAPP:

a) in respect of the verification, processing and approval of CRRs, on a 24*7 basis; and

b) in respect of all other procedures as set out in this SMKI RAPP, on a Working Day basis and during standard working hours in England.

The DCC and any Party, RDP~~, Manufacturer~~ or SECCo may agree that any action taken by either of them prior to the date of the designation of this SMKI RAPP shall, if the equivalent action taken after that date would have satisfied a requirement of this SMKI RAPP for the purposes of appointing a SMKI Registration Authority Manager or member of SMKI Registration Authority Personnel, be treated as if it had taken place after that date.

4. Party, RDP, ~~Manufacturer,~~ SECCo and DCC (as DCC Service Provider) registration procedures

4.1 General registration obligations

4.1.1 Organisation, individual, and RA obligations

Each Party, RDP, ~~Manufacturer,~~ SECCo and the DCC (in its role as DCC Service Provider) shall ensure that its nominated representatives wishing to access SMKI Services and/or the SMKI Repository Service shall undertake the procedures and processes as set out in SMKI RAPP Sections 5.1 to 5.5, as appropriate.

To facilitate this, the SMKI Registration Authority shall:

a) make the forms as set out in SMKI RAPP Annex A, available from the DCC Website or via the DCC SharePoint site as advised by the DCC;

b) provide reasonable support and advice to each Party, RDP, ~~Manufacturer,~~ SECCo and DCC Service Providers in relation to the procedures as set out in SMKI RAPP sections 5.1 to 5.5;

c) place no restriction on the number of individuals that can be nominated as SROs or AROs in respect of any Party, RDP, ~~Manufacturer,~~ SECCo or the DCC (in its role as DCC Service Provider);

d) permit an individual to become an ARO to represent multiple parties, by successfully completing the procedures in SMKI RAPP section 5.3 and 5.4 as are necessary;

e) store and maintain records relating to the nomination, verification and authorisation of individuals and organisations (but not the personal details of individuals) as set out Sections 5.1 to 5.5, and in accordance with the Code and the DCC's data retention policy and data protection policy;

f) not permit any nominated individual to access the SMKI Services or relevant the SMKI Repository Service on behalf of a Party, RDP, ~~Manufacturer,~~ SECCo or the DCC (in its role as DCC Service Provider) until they have become an ARO;

g) ensure that credentials issued under the IKI Certificate Policy to AROs have a lifetime of ten years and that such credentials and shall cease to be valid after ten years following issuance;

h) for authentication and file signing credentials issued under the IKI Certificate Policy and where the Key Pair and Certificate Signing Request are both generated by the prospective ARO on a Cryptographic Credential Token during the ARO verification meeting, that the prospective ARO has an opportunity to validate and agree information (e.g. role and other organisation and individual identity) against which the Certificate is Issued is accurate and that it reflects the identity of the ARO or system that is the subject of the Certificate;

i) for authentication and file signing credentials issued under the IKI Certificate Policy and which are delivered to the SMKI Registration Authority in the form of a Certificate Signing Request generated by the prospective ARO's organisation and provided by the prospective ARO during the ARO verification meeting, that the prospective ARO has an opportunity to validate the information in the resulting Certificate reflects that provided in the Certificate Signing Request and that it is accurate and reflects the identity of the prospective ARO or system that is the subject of the Certificate;

j) for authentication credentials not issued under the IKI Certificate Policy, shall ensure that such authentication credentials remain valid until revoked; and

k) produce, each month, and make available to each Party, RDP~~, Manufacturer~~ and SECCo, a report for that organisation which details the list of SROs, AROs, the credentials that have been issued to each ARO and those AROs for which credentials will expire in the following month.

4.1.2 High level overview of SMKI Registration Authority procedures

Figure 1 as set out immediately below provides a high level view of the procedures required in order for a Party, RDP, ~~Manufacturer,~~ SECCo or the DCC (in its role as DCC Service Provider) to:

- verify their organisational identity;
- become an SRO;
- become an ARO;
- gain credentials for accessing SMKI Services and/or the SMKI Repository Service;
- become an Authorised Subscriber for:
- Organisation Certificates or Device Certificates, or both;

- a File Signing Certificate (issued under the IKI Certificate Policy) for the purposes of verifying Digital Signatures of files in accordance with the Code;

- gain access to Organisation Certificates and/or Device Certificates and other material via the SMKI Repository; and

- gain access to File Signing Certificates, and their corresponding Private Keys to be used for the purposes of Digitally Signing files.

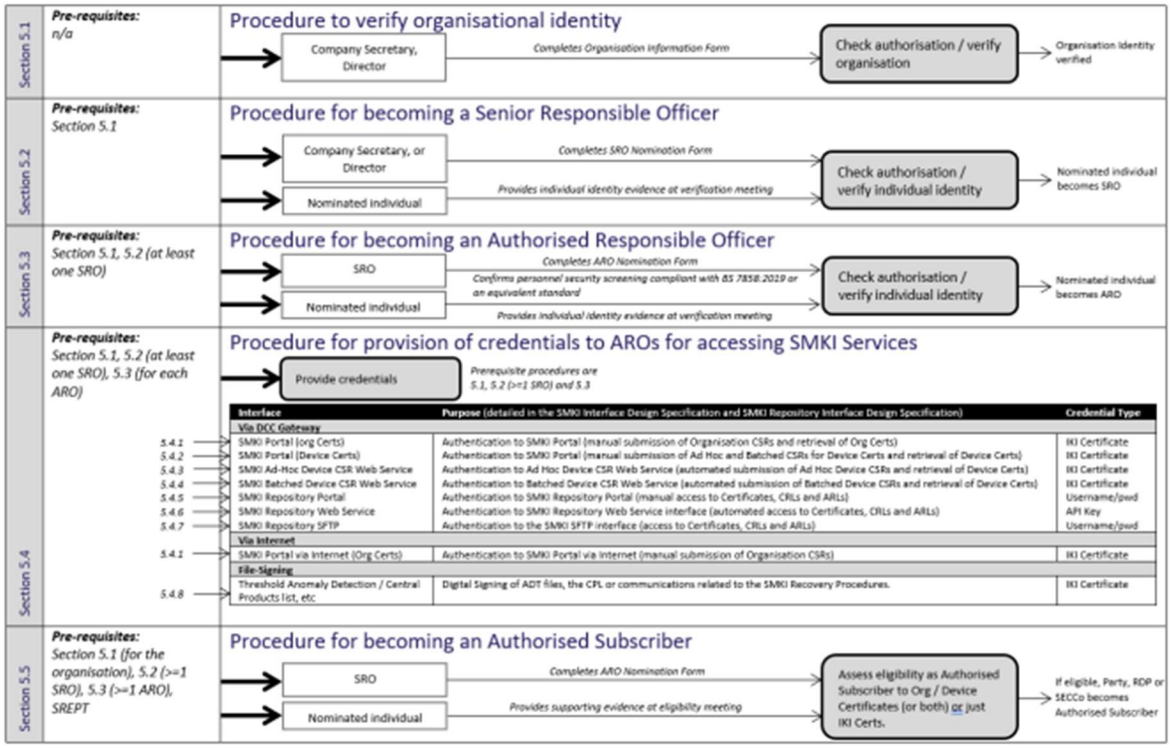

Figure 1: Overview of SMKI access registration processes

- SMKI RAPP Section 5.1 sets out the procedure and detailed processes for confirming the role of the nominating individual and verifying the organisational identity of the Party, RDP, ~~Manufacturer,~~ SECCo or DCC Service Provider, which shall be conducted where its identity has not previously been established.

- SMKI RAPP Section 5.2 sets out the procedure and detailed processes for verifying the identity of an individual nominated to become an SRO. The DCC shall ensure that an individual cannot become an SRO until the organisational identity of the applicant has been verified.

- SMKI RAPP Section 5.3 sets out the procedure and detailed processes for verifying the identity of an individual nominated to become an ARO. The DCC shall ensure that an individual cannot become an ARO until the organisation has at least one SRO and the organisational identity of the applicant has been verified.

- Once an individual has become an ARO, SMKI RAPP Section 5.4 sets out the procedure and detailed processes by which the appropriate credentials used to access SMKI Services and/or the SMKI Repository Service are provided to AROs.

- Where an applicant wishes to be an Authorised Subscriber for Organisation Certificates or Device Certificates or both, Section 5.5 of the SMKI RAPP sets out the procedure and detailed

processes by which the DCC determines if the applicant is eligible to become an Authorised Subscriber for such Organisation Certificates or Device Certificates or both.

In respect of the procedures and detailed processes set out in SMKI RAPP Sections 5.1 to 5.5, the DCC shall place no restriction on the number of forms that can be submitted by an individual Party, RDP, ~~Manufacturer,~~ SECCo or the DCC. Where reasonably practicable, the DCC shall conduct the procedures as set out in SMKI RAPP Sections 5.1 to 5.5 such that where multiple forms are submitted at the same time, multiple procedures can be conducted via a video link by the applicant's nominated individuals.

4.1.3 Change of details

If there is a change to any of the information used to verify the organisational identity of any Party, RDP, Manufacturer, SECCo or a DCC Service Provider (acting on behalf of the DCC), an SRO shall advise the Service Desk of the change and shall ensure that the procedure and detailed processes as set out in SMKI RAPP Section 5.1 is undertaken in respect of the revised evidence of identity, as soon as is reasonably practicable after the change occurs.

If there is a material change to any of the information used to verify the identity of any SRO or ARO, an SRO shall:

a) advise the Service Desk of the change;

b) where required to do so by the SMKI Registration Authority, check the name and address of an ARO before issuing a replacement token, ensure that its SRO or ARO undertakes the procedures as set out in SMKI RAPP Sections 5.2 or 5.3 in respect of the revised evidence of identity, as soon as is reasonably practicable after a material change occurs; and

c) where necessary, for an ARO ensure that credentials used to access SMKI Services and/or the SMKI Repository Service are revoked as set out in SMKI RAPP Section 8.3.

No Party, RDP, ~~Manufacturer,~~ SECCo or the DCC (acting as DCC Service Provider) shall unreasonably withhold information that is required by the SMKI Registration Authority in order to perform the procedures as set out in SMKI RAPP Sections 5.1 to 5.5.

4.1.4 Director or Company Secretary ceasing to be eligible to act on behalf of a Party, RDP~~, Manufacturer~~ or SECCo

Where Director or Company Secretary ceases to be eligible to act on behalf of a Party, RDP~~, Manufacturer~~ or SECCo in respect of the procedures set out in the SMKI RAPP:

a) the Director or Company Secretary themselves, or a Senior Responsible Officer (SRO) whose identity has previously been verified by the DCC, shall advise the Service Desk of the change;

b) the DCC shall confirm such information from the relevant Nominee Details Form, in order to provide confidence that the request is from a Director, Company Secretary or SRO; and

c) if b) is successful, the DCC shall update the DCC's records of authorised individuals for the Party, RDP~~, Manufacturer~~ or SECCo and shall no longer consider the individual to be able to act on behalf of that Party, RDP~~, Manufacturer~~ or SECCo.

4.1.5 SROs ceasing to be eligible to act on behalf of a Party, RDP~~, Manufacturer~~ or SECCo

Where an SRO ceases to be eligible to act on behalf of a Party, RDP~~, Manufacturer~~ or SECCo in respect of the procedures set out in the SMKI RAPP:

a) the SRO themselves, or a Director, Company Secretary or SRO whose identity has previously been verified by the DCC, shall advise the Service Desk of the change;

b) the DCC shall confirm such information from the relevant Nominee Details Form, in order to provide confidence that the request is from an SRO, Director or Company Secretary; and

c) if b) is successful, update the DCC's records of authorised individuals for the Party, RDP~~, Manufacturer~~ or SECCo and shall no longer consider the individual to be able to act on behalf of that Party, RDP~~, Manufacturer~~ or SECCo.

5. Detailed Party, RDP, ~~Manufacturer,~~ SECCo and DCC (as DCC Service Provider) registration procedures and processes

Each Party, RDP, ~~Manufacturer,~~ SECCo and DCC (in its role as DCC Service Provider) shall ensure that its nominated representatives wishing to access SMKI Services and/or the SMKI Repository Service shall undertake the procedures and processes as set out in SMKI RAPP Sections 5.1 to 5.5, as appropriate.

5.1 Procedure and processes to verify organisational identity

The processes as detailed immediately below shall be conducted by the SMKI Registration Authority in order to verify the organisational identity of a Party, RDP, ~~Manufacturer,~~ SECCo or DCC Service Provider (acting on behalf of the DCC).

Step	When	Obligation	Responsibility	Next Step
5.1.1	As required	The applicant organisation shall complete the Organisation Information Form, as set out in SMKI RAPP Annex A (A1). In doing so, the applicant organisation shall ensure that: a. the information entered on the form is complete and accurate; b. the EUI-64 Compliant identifier range for any particular User Role is defined by the applicant organisation such that the range is continuous and does not overlap with the EUI-64 Compliant identifier range for any other User Role, other than where a particular EUI64 Compliant identifier is allowed to be used for more than one	Director or Company Secretary, on behalf of the applicant organisation, which shall be a Party, RDP, ~~Manufacturer,~~ SECCo or DCC Service Provider	5.1.2

		User Role in accordance with H1.5; and c. the Organisation Information Form is authorised by a Director or Company Secretary on behalf of the applicant organisation. The applicant organisation shall also complete the Nominee Details Form, as set out in SMKI RAPP Annex A (A5), for the Director or Company Secretary that has authorised the Organisation Information Form. In doing so, the applicant organisation shall ensure that the information entered on the form is complete and accurate.		
5.1.2	As required following 5.1.1	Submit the completed Organisation Information Form and Nominee Details Form to the SMKI Registration Authority, in writing, as directed on the DCC Website.	Director or Company Secretary, on behalf of the applicant organisation, which shall be a Party, RDP, ~~Manufacturer,~~ SECCo or DCC Service Provider.	5.1.3
5.1.3	As soon as reasonably practicable following receipt of completed Organisation Information Form	Acknowledge receipt by email to the Director or Company Secretary that has authorised the Organisation Information Form.	Service Desk	5.1.4
5.1.4	As soon as reasonably practicable following 5.1.3	Confirm that the nominating Director or Company Secretary holds such a position within the application	SMKI Registration Authority Personnel	If complete, accurate and no discrepancies, 5.1.6; if not complete and

		organisation, via a public information source. Analyse the information entered on the Organisation Information Form and Nominee Details Form, to determine completeness, discrepancies and whether the submitted EUI64 Compliant identifier ranges are consistent with the restriction set out in step 5.1.1. Where there are omissions/discrepancies or the submitted identifier ranges are not consistent with the restriction set out in step 5.1.1, the SMKI Registration Authority shall agree actions and/or amendments, via email, with the Director or Company Secretary that has authorised the Organisation Information Form.		accurate or any discrepancies, 5.1.5
5.1.5	Once omissions / discrepancies addressed	Submit a revised Organisation Information Form and/or Nominee Details Form to the SMKI Registration Authority, or in writing as directed on the DCC Website.	Director or Company Secretary, on behalf of the applicant organisation, which shall be a Party, RDP, ~~Manufacturer,~~ SECCo or DCC Service Provider	5.1.3
5.1.6	As soon as reasonably practicable, following 5.1.4	Agree with the applicant organisation and confirm, by email, the date and time of a meeting to verify the organisation identity to the Director, or Company Secretary that has signed the Organisation Information Form. The meeting shall be	SMKI Registration Authority	5.1.7

		held via a video link or face to face if preferred.		
5.1.7	As soon as reasonably practicable on becoming aware of unavailability	If it is identified that SMKI Registration Authority Personnel will be unavailable to conduct the verification meeting on the agreed date and time, the SMKI Registration Authority shall inform the applicant Director or Company Secretary by email, and shall agree and confirm an alternative date and time. If it is identified that the individual(s) acting on behalf of the applicant organisation will be unavailable to attend the verification meeting on the agreed date and time, the individual(s) shall inform the SMKI Registration Authority, by email, and shall agree and confirm an alternative date and time.	SMKI Registration Authority or applicant organisation, as appropriate	5.1.8
5.1.8	In meeting to verify organisational identity	Verify: a. the organisational identity of the applicant organisation to the level pursuant to the SMKI PMA Guidance on "Verifying Organisation Identity" published on the Website; b. via information held by SECCo, that the applicant organisation has the User Role or User Roles as specified in Organisation Information Form; c. proof of individual identity provided for the nominating individual against the information	SMKI Registration Authority Personnel	If not successful, 5.1.9; if successful, 5.1.10

		listed on the Organisation Information Form and the Nominee Details Form; and d. the individual identity of the nominating individual to the level pursuant to the SMKI PMA Guidance on "Verifying Individual Identity" published on the Website.		
5.1.9	As soon as reasonably practicable, following 5.1.8	If verification in 5.1.8 is unsuccessful, notify the nominating Director, Company Secretary or SRO that verification of the organisational identity has been unsuccessful, by email.	SMKI Registration Authority Personnel	5.1.5 once issues addressed
5.1.10	As soon as reasonably practicable, following 5.1.8	If verification in 5.1.8 is successful, inform the nominating Director or Company Secretary that the organisational identity has been successfully verified, by email.	SMKI Registration Authority	5.1.11
5.1.11	As soon as reasonably practicable, following 5.1.10	Add the verified organisation to the DCC's list of such organisations, in accordance with Section 4.1.2 (A) (ii) of Appendix A to the Code and Section 4.1.2 (A) (ii) of Appendix B to the Code.	SMKI Registration Authority	End of procedure

5.2 Procedure for becoming a Senior Responsible Officer

The procedure as detailed immediately below shall be conducted by the SMKI Registration Authority in order to check the authorisation and verify the identity of any individual that has been nominated to become a Senior Responsible Officer in respect of that Party, RDP, ~~Manufacturer,~~ SECCo or the DCC (in its role as DCC Service Provider).

Step	When	Obligation	Responsibility	Next Step
5.2.1	As required	Complete the SMKI SRO Nomination Form and	Director or Company Secretary, on behalf	5.2.2

		Nominee Details Form, as set out in SMKI RAPP Annex A (A3) and Annex A (A5). In doing so, the individual completing the SMKI SRO Nomination Form and Nominee Details Form shall ensure that the information entered on the forms is complete and accurate, and that: a. the nominating individual is for a Party, RDP, ~~Manufacturer,~~ SECCo or the DCC (as DCC Service Provider), a Director of, or Company Secretary of and an employee of, the applicant organisation or its parent organisation; and b. the SMKI SRO Nomination Form and Nominee Details Form are both authorised, where applicable, by a Director or Company Secretary on behalf of the applicant organisation. entered on the form is complete and accurate.	of the applicant organisation, which shall be a Party, RDP, ~~Manufacturer,~~ SECCo or DCC (as DCC Service Provider).	
5.2.2	As required, following 5.2.1	Submit the completed SMKI SRO Nomination Form and Nominee Details Form to the SMKI Registration Authority, in writing, as directed on the DCC Website.	Director or Company Secretary, on behalf of the applicant organisation, which shall be a Party, RDP, ~~Manufacturer,~~ SECCo or DCC (as DCC Service Provider).	5.2.3
5.2.3	As soon as reasonably practicable following receipt of completed	Acknowledge receipt to the Director or Company Secretary that has authorised the SMKI SRO Nomination Form.	Service Desk	5.2.4

	SRO Nomination Form			
5.2.4	As soon as reasonably practicable following 5.2.3	Analyse the information entered on the SMKI SRO Nomination Form and Nominee Details Form, to: a. determine completeness and any discrepancies; and b. confirm, using the DCC's records or using publicly available information, that the Director or Company Secretary that has authorised the SMKI SRO Nomination Form has the role indicated on the SMKI SRO Nomination Form. Where there are omissions/discrepancies, agree actions with the nominating individual, via email.	SMKI Registration Authority Personnel	If complete, 5.2.6; if not complete, 5.2.5
5.2.5	Once omissions / discrepancies addressed	Submit a revised SMKI SRO Nomination Form and/or Nominee Details Form to the SMKI Registration Authority, in writing as directed on the DCC Website.	Director or Company Secretary, on behalf of the applicant organisation, which shall be a Party, RDP, ~~Manufacturer,~~ SECCo or DCC (as DCC Service Provider).	5.2.3
5.2.6	As soon as reasonably practicable, following 5.2.4	If the SMKI Registration Authority has any questions about the information submitted, contact the Director or Company Secretary that nominated the individual, via telephone, using the telephone number provided previously in the SMKI SRO Nomination Form,	SMKI Registration Authority Personnel	If confirmed as authorised, 5.2.8; if not confirmed as authorised, 5.2.7

		to confirm whether each nominated individual on the SMKI SRO Nomination Form is authorised to act on behalf of the organisation as SRO and seek confirmation of information provided on the SMKI SRO Nomination Form in order to provide confidence that the correct person has been contacted.		
5.2.7	As soon as reasonably practicable following rejection	Inform the applicant organisation that the application to become a Senior Responsible Officer has not been successful, by email to the Director or Company Secretary that has authorised the SMKI SRO Nomination Form.	SMKI Registration Authority Personnel	5.2.6 once issues resolved
5.2.8	As soon as reasonably practicable, following 5.2.6	Agree, via email with the individual nominated to become a Senior Responsible Officer, a date and time for the nominated individual(s) to attend a face to face verification meeting in person or by video link.	SMKI Registration Authority Personnel	5.2.9
5.2.9	As soon as reasonably practicable on becoming aware of unavailability	If it is identified that SMKI Registration Authority Personnel will be unavailable to conduct the verification meeting on the agreed date and time, the SMKI Registration Authority shall inform the nominated individual, and shall agree and confirm an alternative date and time. If it is identified that the individual(s) nominated to act on behalf of the applicant organisation will be unavailable to attend the verification meeting on the agreed date and time, the nominated individual shall	SMKI Registration Authority or applicant organisation, as appropriate	5.2.10

		inform the SMKI Registration Authority, by email and telephone, and shall agree and confirm an alternative date and time.		
5.2.10	In SRO verification meeting	At the face-to-face SRO verification meeting in person or by video link, the SMKI Registration Authority shall, in person: a. check proof of individual identity provided for each nominated individual against the information listed on the SRO Nomination Form and the Nominee Details Form; and b. verify the individual identity for each nominated individual to the level pursuant to the SMKI PMA Guidance on "Verifying Individual Identity" published on the Website.	SMKI Registration Authority	If not successfully verified, 5.2.11; if successfully verified, 5.2.12
5.2.11	As soon as reasonably practicable, following verification meeting	Notify the Director or Company Secretary in writing, that the nominated individual(s) has not been verified successfully and has not become a Senior Responsible Officer on behalf of the applicant organisation.	SMKI Registration Authority	5.2.5 once issues addressed
5.2.12	As soon as reasonably practicable, following verification meeting	Notify the Director or Company Secretary in writing, that the nominated individual(s) has become a Senior Responsible Officer on behalf of the applicant organisation.	SMKI Registration Authority	5.2.13
5.2.13	As soon as reasonably	Add the relevant SRO to the DCC's list of SROs, in accordance with Section 4.1.2 (A) (ii) of Appendix A to the	SMKI Registration Authority	End of Procedure

	practicable, 5.2.12	Code and Section 4.1.2 (A) (ii) of Appendix B to the Code.		

5.3 Procedure for becoming an Authorised Responsible Officer

The procedure as detailed immediately below shall be conducted by the SMKI Registration Authority in order to check the authorisation and verify the identity of any individual that has been nominated to become an Authorised Responsible Officer in respect of that Party, RDP, ~~Manufacturer,~~ SECCo or the DCC (in its role as DCC Service Provider).

Step	When	Obligation	Responsibility	Next Step
5.3.1	As required	Complete the SMKI ARO Nomination Form and Nominee Details Form as set out in SMKI RAPP Annex A (A4) and Annex A (A5), ensuring that: a. the information entered on the forms is complete and accurate; b. the SMKI ARO Nomination Form and Nominee Details Form are authorised by an SRO on behalf of the applicant organisation; and c. the SRO has confirmed that the SMKI ARO Nominee has been subject to a standard that is compliant with BS 7858:2019 or an equivalent standard.	SRO on behalf of the applicant organisation, which shall be a Party, RDP, ~~Manufacturer,~~ SECCo or DCC (as DCC Service Provider).	5.3.2
5.3.2	As required, following 5.3.1	Submit the completed SMKI ARO Nomination Form and Nominee Details Form to the SMKI Registration Authority in writing, as directed on the DCC Website.	SRO on behalf of the applicant organisation, which shall be a Party, RDP, ~~Manufacturer,~~ SECCo or DCC (as DCC Service Provider)	5.3.3
5.3.3	As soon as reasonably	Acknowledge receipt by email to the SRO as identified on	Service Desk	5.3.4

	practicable following receipt of completed ARO Nomination Form and Nominee Details Form	the SMKI ARO Nomination Form.		
5.3.4	As soon as reasonably practicable following 5.3.3	Analyse the information entered on the SMKI ARO Nomination Form and Nominee Details Form; determine completeness and any discrepancies. Where there are omissions/discrepancies, agree actions with the SRO via email.	SMKI Registration Authority	If complete, 5.3.6; if not complete, 5.3.5
5.3.5	Once omissions / discrepancies are addressed	Submit a revised SMKI ARO Nomination Form and/or Nominee Details Form to the Registration Authority in writing as directed on the DCC Website.	SRO on behalf of the applicant organisation, which shall be a Party, RDP, ~~Manufacturer,~~ SECCo or DCC (as DCC Service Provider)	5.3.3
5.3.6	As soon as reasonably practicable, following 5.3.4	If the SMKI Registration Authority has any questions about the information submitted, contact an SRO of the applicant organisation via telephone, using the registered contact information for the SRO as held by the SMKI Registration Authority, to confirm whether the nominated individual is authorised to become an ARO.	SMKI Registration Authority	If confirmed as authorised, 5.3.8; if not authorised, 5.3.7
5.3.7	As soon as reasonably practicable	Notify the individual and an SRO that the procedure for becoming an ARO has not been successful for relevant	SMKI Registration Authority	5.3.5 once issues addressed

	following rejection	nominated individual, by email.		
5.3.8	As soon as reasonably practicable, following 5.3.6	Agree with the applicant organisation and confirm the date and time for the ARO verification meeting, via email to the nominated individual and an SRO of the applicant organisation.	SMKI Registration Authority	5.3.9
5.3.9	As soon as reasonably practicable on becoming aware of unavailability	If it is identified that SMKI Registration Authority Personnel will be unavailable to conduct the verification meeting on the agreed date and time, the SMKI Registration Authority shall inform an SRO and the nominated individual, by email, and shall agree and confirm an alternative date and time. If it is identified that the nominated individual(s) acting on behalf of the applicant organisation will be unavailable to attend the verification meeting on the agreed date and time, an SRO shall inform the SMKI Registration Authority, by email, and shall agree and confirm an alternative date and time.	SMKI Registration Authority or applicant organisation, as appropriate	5.3.10
5.3.10	In ARO verification meeting	At the ARO face-to-face verification meeting, the SMKI Registration Authority shall, in person, for the nominated individual: a. check proof of individual identity provided against the information listed on the ARO Nomination Form and Nominee Details Form; and	SMKI Registration Authority	If verified, 5.3.12; if not verified, 5.3.11

		b. verify the identity of the nominated individual to the level pursuant to the SMKI PMA Guidance on "Verifying Individual Identity" published on the Website.		
5.3.11	As soon as reasonably practicable, following ARO verification meeting	Notify: a. the nominated individual that they have become an ARO, verbally; or b. in writing to the SRO, that the verification has not been successful for the nominated individual, that the nominated individual has not become an ARO, and provide reasons for the rejection and request that the nominated individual is required to attend a further ARO verification meeting once the issues have been remedied.	SMKI Registration Authority	If successful, 5.3.12; otherwise 5.3.5 once issues are addressed
5.3.12	As soon as reasonably practicable, following ARO verification meeting	Ensure that the applicant organisation is notified of the individuals whose identity has been verified and have become AROs by email or via the Service Desk updating the relevant ticket, ensuring that there is a record for audit purposes.	SMKI Registration Authority or Service Desk	5.3.13
5.3.13	As soon as reasonably practicable, following 5.3.12	Add the relevant individual to the DCC's list of AROs, in accordance with Section 4.1.2 (A) (ii) of Appendix A to the Code and Section 4.1.2 (A) (ii) of Appendix B to the Code.	SMKI Registration Authority	Procedure as set out in SMKI RAPP section 5.5

5.4 Procedure for provision of credentials to AROs for accessing SMKI Services and the SMKI Repository Service and file signing

The procedure and processes as detailed immediately below shall be conducted by the SMKI Registration Authority in order to provide credentials for accessing SMKI Services and/or the SMKI Repository Service or for file signing to Authorised Responsible Officers in respect of a Party, RDP, ~~Manufacturer,~~ SECCo or the DCC (in its role as DCC Service Provider). The SMKI Registration Authority shall not provide such credentials to an individual on behalf of a Party, RDP, ~~Manufacturer,~~ SECCo or the DCC (in its role as DCC Service Provider), other than where the organisation has completed SMKI and Repository Entry Process Tests and such individuals have become Authorised Responsible Officers.

Step	When	Obligation	Responsibility	Next Step
5.4.1	During ARO verification meeting and after becoming an ARO	**IKI credentials for submission of CSRs in respect of Organisation Certificates using SMKI Portal via DCC Gateway Connection or SMKI Portal via the Internet** If the applicant has indicated on the Authorised Subscriber application form that it wishes to be an Authorised Subscriber for Organisation Certificates and/or Device Certificates, and where the Party, RDP, ~~Manufacturer,~~ SECCo or DCC Service Provider has successfully completed SMKI and Repository Entry Process Tests, the SMKI Registration Authority shall, if the ARO wishes to access the SMKI Portal interface, provide the ARO with: a. If the applicant organisation has access to a DCC Gateway Connection, one Cryptographic Credential Token containing credentials issued under the applicable IKI Certification Authority that authenticate the ARO to access the SMKI Portal Interface for the purposes of submission of CSRs in respect of Organisation Certificates and retrieval of	SMKI Registration Authority	5.4.2

		corresponding Organisation Certificates via a DCC Gateway Connection. The DCC shall ensure that the Cryptographic Credential Token enables the ARO to set a PIN code which shall be used each time the Cryptographic Credential Token is used, to render the Cryptographic Credential Token operative. Such credentials shall not allow the ARO to access the SMKI Portal Interface via the Internet. b. If the applicant organisation does not have access to a DCC Gateway Connection, one Cryptographic Credential Token containing credentials issued under the applicable IKI Certification Authority that authenticate the ARO to access the SMKI Portal Interface via the Internet for the purposes of submission of CSRs in respect of Organisation Certificates and retrieval of corresponding Organisation Certificates. The DCC shall ensure that the Cryptographic Credential Token enables the ARO to set a PIN code which shall be used each time the Cryptographic Credential Token is used, to render the Cryptographic Credential Token operative. Such credentials shall not allow the ARO to access the SMKI Portal		

		Interface via a DCC Gateway Connection. Where the Party, RDP, ~~Manufacturer,~~ SECCo or DCC (in its role as DCC Service Provider) has not successfully completed SMKI and Repository Entry Process Tests, the DCC shall retain such Cryptographic Credential Token until such time as the Party, RDP, ~~Manufacturer,~~ SECCo or DCC (as DCC Service Provider) has successfully completed SMKI and Repository Entry Process Tests, at which point the DCC shall send such Cryptographic Credential Token to the ARO via secure courier.		
5.4.2	During ARO verification meeting and after becoming an ARO	**IKI credentials for submission of CSRs in respect of Device Certificates using SMKI Portal via DCC Gateway Connection** If the applicant has indicated on the Authorised Subscriber application form that it wishes to be an Authorised Subscriber for Device Certificates, the Registration Authority shall determine, in accordance with the steps set out in Section 5.5 of the SMKI RAPP, whether there is reasonable evidence to suggest that it is necessary for the applicant organisation to become an Authorised Subscriber for Device Certificates in order for them to carry out business processes that will, or are likely to, lead to the installation of Devices in premises. Where	SMKI Registration Authority	5.4.3

		there is such reasonable evidence, and where the applicant organisation has successfully completed SMKI and Repository Entry Process Tests, the SMKI Registration Authority shall, if the ARO wishes to access the SMKI Portal Interface, provide the ARO with: a. If the applicant organisation has access to a DCC Gateway Connection, one Cryptographic Credential Token containing credentials issued under the applicable IKI Certification Authority that authenticate the ARO to access the SMKI Portal Interface for the purposes of submission of CSRs in respect of Device Certificates and retrieval of corresponding Device Certificates via a DCC Gateway Connection. The DCC shall ensure that the Cryptographic Credential Token enables the ARO to set a PIN code which shall be used each time the Cryptographic Credential Token is used, to render the Cryptographic Credential Token operative. Such credentials shall not allow the ARO to access the SMKI Portal Interface via the Internet. Where the Party, RDP or DCC (in its role as DCC Service Provider) has not successfully completed SMKI and Repository Entry Process		

		Tests, the DCC shall retain such Cryptographic Credential Token until such time as the Party, RDP or DCC (as DCC Service Provider) has successfully completed SMKI and Repository Entry Process Tests, at which point the DCC shall send such Cryptographic Credential Token to the ARO via secure courier.		
5.4.3	During ARO verification meeting and after becoming an ARO	**IKI credentials for Ad Hoc Device CSR Web Service** If the applicant has indicated on the Authorised Subscriber application form that it wishes to be an Authorised Subscriber for Device Certificates and it wishes to use the Ad Hoc Device CSR Web Service, the SMKI Registration Authority shall, if the applicant organisation has access to a DCC Gateway Connection and is a Supplier Party or the DCC, and where the Supplier Party or DCC (in its role as DCC Service Provider) has successfully completed SMKI and Repository Entry Process Tests, the SMKI Registration Authority shall provide the ARO, via USB token or optical media, with Ad Hoc Device CSR Web Service access credentials for Device Certificates, which corresponds with a CSR that shall be provided, via USB token or optical media, by the applicant organisation in accordance with the SMKI Interface Design Specification, sections 2.4 xv, xvi & xvii. If the Supplier Party or DCC (in its role as DCC Service	SMKI Registration Authority	5.4.4

		Provider) has not successfully completed SMKI and Repository Entry Process Tests at the time of the verification meeting, once the Supplier Party or DCC (as DCC Service Provider) has successfully completed SMKI and Repository Entry Process Tests, the SMKI Registration Authority shall provide, on a USB token or optical media via secure courier or by secured electronic means, the appointed ARO with Ad Hoc Device CSR Web Service access credentials for Device Certificates, which corresponds with a CSR that shall be provided by the applicant organisation in accordance with the SMKI Interface Design Specification.		
5.4.4	During ARO verification meeting and after becoming an ARO	**IKI credentials for Batched Device CSR Web Service** If the applicant has indicated on the Authorised Subscriber application form that it wishes to be an Authorised Subscriber for Device Certificates and it wishes to use the Batched Device CSR Web Service, the SMKI Registration Authority shall determine, if the applicant organisation has access to a DCC Gateway Connection and the applicant is not a Supplier Party or the DCC, in accordance with the steps set out in Section 5.5 of the SMKI RAPP, whether there is reasonable evidence to suggest that it is necessary for the applicant organisation to become an Authorised Subscriber for Device	SMKI Registration Authority	5.4.5

		Certificates in order for them to carry out business processes that will, or are likely to, lead to the installation of Devices in premises. Where there is such reasonable evidence, and where the applicant organisation has successfully completed SMKI and Repository Entry Process Tests, the SMKI Registration Authority shall provide the appointed ARO, via USB token or optical media, with Batched Device CSR Web Service access credentials for Device Certificates, which shall be Issued by the DCC in response to a valid CSR that shall be provided by the applicant organisation in accordance with the SMKI Interface Design Specification, sections 2.5 xxvi & xxvii. If the applicant organisation has not successfully completed SMKI and Repository Entry Process Tests at the time of the verification meeting, once the applicant organisation has successfully completed SMKI and Repository Entry Process Tests, the SMKI Registration Authority shall provide, on a USB token or optical media via secure courier or by secured electronic means, the appointed ARO with Batched Device CSR Web Service access credentials for Device Certificates, which corresponds with a CSR that shall be provided by the applicant organisation in accordance with the SMKI Interface Design Specification.		

5.4.5	During ARO verification meeting and after becoming an ARO	**Credentials for SMKI Repository portal** If the applicant organisation has access to a DCC Gateway Connection, and it wishes to access the SMKI Repository via the SMKI Repository Portal and has successfully completed SMKI and Repository Entry Process Tests, provide the appointed ARO with a username and password, to be accessed via the SMKI Repository Portal, that is specific to the Authorised Responsible Officer, for the purposes of authenticating to the SMKI Repository Portal via DCC Gateway Connection, as set out in the SMKI Repository Interface Design Specification, section 2.1.2. If the applicant organisation has access to a DCC Gateway Connection, it wishes to access the SMKI Repository via the SMKI Repository Portal but has not successfully completed SMKI and Repository Entry Process Tests at the time of the verification meeting: a. DCC shall, once the applicant organisation has successfully completed SMKI and Repository Entry Process Tests, provide the appointed ARO with a username and password via secured electronic means that is specific to the Authorised Responsible Officer, for the purposes of authenticating to the SMKI Repository Portal via DCC Gateway Connection, as set out in	SMKI Registration Authority	5.4.6

		the SMKI Repository Interface Design Specification, section 2.1.2.		
5.4.6	During ARO verification meeting and after becoming an ARO	**Credentials for SMKI Repository web service** If the applicant organisation has access to a DCC Gateway Connection, and wishes to access the SMKI Repository Web Service interface and has successfully completed SMKI and Repository Entry Process Tests, provide the ARO with the credentials required to authenticate to the SMKI Repository Web Service interface, as set out in the SMKI Repository Interface Specification section 2.2.1, along with a certificate which enables verification of the SMKI Repository Web Service server identity. If the applicant organisation has access to a DCC Gateway Connection, wishes to access the SMKI Repository Web Service interface but has not successfully completed SMKI and Repository Entry Process Tests at the time of the verification meeting, once the applicant organisation has successfully completed SMKI and Repository Entry Process Tests, the SMKI Registration Authority shall provide, on electronic media as set out in the "SMKI Repository User Guide", the ARO with the credentials required to authenticate to the SMKI Repository Web Service interface, as set out in the SMKI Repository Interface	SMKI Registration Authority	5.4.7

		Design Specification section 2.2.1.		
5.4.7	During ARO verification meeting and after becoming an ARO	Credentials for SMKI Repository Portal SFTP If the applicant organisation has access to a DCC Gateway Connection, wishes to access the SMKI Repository using SSH File Transfer Protocol (SFTP) access credentials and has successfully completed SMKI and Repository Entry Process Tests, provide the ARO with credentials, in the form of a username and password, used to access the SSH File Transfer Protocol (SFTP) interface, as set out in the SMKI Repository Interface Design Specification section 2.3.1. If the applicant organisation has access to a DCC Gateway Connection, wishes to access the SMKI Repository using SSH File Transfer Protocol (SFTP) access credentials but has not successfully completed SMKI and Repository Entry Process Tests at the time of the verification meeting, once the applicant organisation has successfully completed SMKI and Repository Entry Process Tests, the SMKI Registration Authority shall provide the ARO, via the SMKI Repository Portal profile page, with credentials, in the form of a username and password, used to access the SSH File Transfer Protocol (SFTP) interface, as set out in the SMKI Repository Interface Design Specification section 2.3.1.	SMKI Registration Authority	5.4.8

5.4.8	During ARO verification meeting and after becoming an ARO	**IKI credentials for file signing** If the applicant organisation wishes the ARO to be Issued with a File Signing Certificate for the purposes as set out in the Code, the SMKI Registration Authority shall either: a. provide the ARO with a Cryptographic Credential Token enabling the ARO to submit a CSR for a File Signing Certificate; in which case, the ARO shall use the software on the Cryptographic Credential Token to generate a Private Key for a File Signing Certificate to submit a CSR for a File Signing Certificate; and if the CSR is valid, the ICA shall Issue a File Signing Certificate under the IKI Certificate Policy, to be used for the purposes as set out in the Code; or b. provide the appointed ARO, via USB token or optical media, with an IKI File Signing Certificate, which shall be Issued by the DCC in response to a valid CSR that shall be provided by the applicant organisation.	SMKI Registration Authority	5.4.9
5.4.9	During ARO verification meeting and after issuance of credentials	**Acceptance of credentials issued in steps 5.4.1 to 5.4.8** The SMKI Registration Authority shall complete the relevant sections of the Nominee Details Form in Annex A (A5) accordingly to	SMKI Registration Authority ARO	End of procedure

		confirm credential issuance either manually or digitally and give the form to the ARO, retaining a copy of the original. The ARO shall confirm receipt of and acceptance of the credentials issued by completing the relevant sections of the Nominee Details Form in Annex A (A5) either manually or digitally. The SMKI Registration Authority shall retain a copy of the receipt. Should the ARO not wish to accept these credentials, the ARO shall notify the SMKI Registration Authority immediately and not sign for the Certificate and / or Cryptographic Credential.		

8.3 Revocation of SMKI Services and / or the SMKI Repository Service access credentials and / or IKI File Signing Certificates

8.3.1 General obligations relating to revocation of ARO credentials for accessing SMKI Services and / or the SMKI Repository Service and / or File Signing Certificates

A Senior Responsible Officer on behalf of a Party, RDP, ~~Manufacturer,~~ SECCo or the DCC (in its role as DCC Service Provider) may request the revocation of access credentials in respect of an Authorised Responsible Officer acting on behalf of that Party, RDP, ~~Manufacturer,~~ SECCo or the DCC (as DCC Service Provider) or revocation of an IKI File Signing Certificate for which that Party, RDP, ~~Manufacturer,~~ SECCo is an Authorised Subscriber, using the form as set out in Annex A (A7) and clearly identifying the credentials to be revoked.

The permitted reasons for revocation of authentication credentials shall be as listed immediately below:

a) An applicant wishes an IKI File Signing Certificate or the credentials of an ARO to be revoked.

b) A Party, RDP, ~~Manufacturer,~~ SECCo or the DCC (as DCC Service Provider), of which the ARO is a representative, becomes ineligible to access SMKI Services and/or the SMKI Repository Service or ceases to become an Authorised Subscriber for Device Certificates or Organisation Certificates, or both, as appropriate.

c) If there is a change to any of the information that was used to verify the identity of an ARO (but where the renewal or replacement of documents used to verify such identity, where the identity information remains the same, shall not constitute a change).

d) A Party, RDP, ~~Manufacturer,~~ DCC (as DCC Service Provider), or SECCo notifies the SMKI Registration Authority that it reasonably believes that the ARO is a threat to the security, integrity, or stability of the SMKI Services and/or the SMKI Repository Service.

e) The information on which the identity of an ARO was established is known, or is reasonably suspected, to be inaccurate.

f) The authentication credentials issued to the ARO are lost, stolen, inoperative, or destroyed. The DCC shall ensure that the Cryptographic Credential Token issued to an ARO is automatically rendered inoperative where the PIN code on the Cryptographic Credential Token used to access SMKI Services has been entered incorrectly 15 consecutive times.

Where access credentials have been revoked and the Party, RDP, ~~Manufacturer,~~ SECCo or DCC (as DCC Service Provider) wishes to receive new access credentials, that Party, RDP, ~~Manufacturer,~~ SECCo or DCC (as DCC Service Provider) shall submit a new ARO Nomination Form.

8.3.2 Procedure for revocation of SMKI Services and / or the SMKI Repository Service access credentials for AROs and / or IKI File Signing Certificates

The procedure for verification and, where verified, revocation of authentication credentials or IKI File Signing Certificates is as set out immediately below.

Step	When	Obligation	Responsibility	Next Step
8.3.2.1	As required	Complete the Credential Revocation Request Form as set out in SMKI RAPP Annex A (A7), ensuring that the information entered on the form is complete and accurate, and the Credential Revocation Request Form is authorised by an SRO on behalf of the applicant organisation.	SRO on behalf of the applicant organisation, which shall be a Party, RDP, ~~Manufacturer,~~ SECCo or DCC (as DCC Service Provider)	8.3.2.2
8.3.2.2	As required, following 8.3.2.1	Submit the completed Credential Revocation Request Form to the SMKI Registration Authority via a secured electronic means, as directed on the DCC Website.	SRO on behalf of the applicant organisation, which shall be a Party, RDP, ~~Manufacturer,~~ SECCo or DCC (as DCC Service Provider)	8.3.2.3
8.3.2.3	As soon as reasonably practicable following 8.3.2.2	Acknowledge receipt by email to the SRO as identified on the Credential Revocation Request Form or via the Service Desk updating the relevant ticket, ensuring a record is kept.	SMKI Registration Authority or Service Desk	8.3.2.4
8.3.2.4	As soon as reasonably practicable	Analyse the information entered on the Credential Revocation Request Form;	SMKI Registration Authority	If complete, 8.3.2.6; if not

	following 8.3.2.3	determine completeness and any discrepancies. Where there are omissions/discrepancies, agree actions with an SRO via email.		complete, 8.3.2.5
8.3.2.5	Once omissions / discrepancies are addressed	Submit a revised Credential Revocation Request Form to the SMKI Registration Authority via a secured electronic means, as directed on the DCC Website.	SRO on behalf of the applicant organisation, which shall be a Party, RDP, ~~Manufacturer,~~ SECCo or DCC (as DCC Service Provider)	8.3.2.3
8.3.2.6	As soon as reasonably practicable, following 8.3.2.4	Contact the SRO as identified on the Credential Revocation Request Form, using the registered contact information for the SRO as held by the SMKI Registration Authority, to confirm the application identified by the Credential Revocation Request Form is authorised.	SMKI Registration Authority	If confirmed as authorised, 8.3.2.8; if not authorised, 8.3.2.7
8.3.2.7	As soon as reasonably practicable following rejection	Notify the SRO that was contacted in step 8.3.2.3, that the procedure in respect of the application has not been successful, by email.	SMKI Registration Authority	End of procedure
8.3.2.8	As soon as reasonably practicable following 8.3.2.6	Notify the SRO that was contacted in step 8.3.2.3, and the DCC's CISO by email that the revocation request has been accepted.	SMKI Registration Authority Personnel, on behalf of the SMKI Registration Authority	8.3.2.9
8.3.2.9	As soon as reasonably practicable following 8.3.2.8	Revoke the credentials for the relevant service, for the identified ARO or relevant IKI File Signing Certificate as indicated by the SRO on the Credential Revocation Request Form. In doing so, the DCC shall, where required to revoke the credentials, revoke all associated IKI	SMKI Registration Authority Personnel, on behalf of the SMKI Registration Authority	8.3.2.10

		Certificates. DCC shall ensure that access to the relevant service is prevented from the point of revocation.		
8.3.2.10	As soon as reasonably practicable following 8.3.2.9	Notify the SRO that was contacted in step 8.3.2.3 of the successful revocation of credentials for the ARO or relevant IKI File Signing Certificate. Where such revocation results in the individual that is the subject of the Credential Revocation Request Form no longer having any valid credentials issued to them in accordance with the SMKI RAPP, the SMKI Registration Authority shall notify the SRO that was contacted in step 8.3.2.3 that the individual is no longer an ARO, by email.	SMKI Registration Authority Personnel, on behalf of the SMKI Registration Authority	8.3.2.11
8.3.2.11	As soon as reasonably practicable following 8.3.2.10	Where the revoked credentials were issued on a Cryptographic Credential Token or Cryptographic Credential Tokens, the Party, RDP, ~~Manufacturer,~~ SECCo or DCC Service Provider shall, where such Cryptographic Credential Tokens are in the possession of the applicant organisation, send the Cryptographic Credential Token or Cryptographic Credential Tokens to the DCC, via secure courier.	SRO on behalf of the applicant organisation	8.3.2.12
8.3.2.12	As soon as reasonably practicable following 8.3.2.11	The DCC shall verifiably destroy all Secret Key Material or Certificates contained on the returned Cryptographic Credential Token.	SMKI Registration Authority Manager, on behalf of the SMKI Registration Authority	8.3.2.13

8.3.2.13	As soon as reasonably practicable following 8.3.2.12	Record the details of the credentials that have been revoked in respect of the ARO as identified on the Credential Revocation Request Form or relevant IKI File Signing Certificate, plus, if relevant, update the DCC's list of AROs, in a manner which is auditable.	SMKI Registration Authority	End of procedure

Annex B. Definitions

Authorised Responsible Officer (ARO)	Means an individual that has successfully completed the process for becoming an ARO on behalf of a Party, RDP, ~~Manufacturer,~~ SECCo or a DCC Service Provider in accordance with the SMKI RAPP and/or the DCCKI RAPP (as applicable).
Senior Responsible Officer (SRO)	Means an individual that has successfully completed the process for becoming an SRO on behalf of a Party, RDP, ~~Manufacturer,~~ SECCo or a DCC Service Provider in accordance with the SMKI RAPP and/or the DCCKI RAPP (as applicable).

APPENDIX Z

CPL Requirements Document

Contents

1. Overview……2
2. Central Products List Contents……2
3. Addition of Device Models to the List……3
4. Association of Hashes with Device Models on the CPL……4
5. Adding Device Models to CPA Certificates……5
6. Removal of Device Models from the List……5
7. Digital Signatures on CPL……....7

1. Overview

1.1 This Appendix supplements Section F2 (Central Products List).

2. Central Products List Contents

2.1 The Panel shall ensure that the Central Products List identifies each Device Model by Physical Device Type, and lists the following matters in respect of each Device Model:

(a) Manufacturer and model;

(b) hardware version;

(c) firmware version;

(d) for SMETS2+ Device Models, the version of the SMETS or CHTS (as applicable) and (in each case) the GBCS version for which the Device Model has one or more Assurance Certificates;

(e) for SMETS1 Device Models, Version 1.2 of SMETS;

(f) for SMETS2+ Device Models, the identification numbers for each of the Device Model's Assurance Certificates (including the version of the relevant standard against which each Assurance Certificate was issued);

(g) where the Device Model is required to have an associated CPA Certificate, the expiry or renewal date of the Device Model's CPA Certificate and the associated

version of the Security Characteristics (as defined in the relevant Technical Specification); and

(h) where there is an associated Manufacturer Image:

(i) the relevant identity of the person who created the Manufacturer Image;

(ii) a descriptor of the Manufacturer Image; and

(iii) the Hash of the Manufacturer Image (to be provided pursuant to Clause 4).

3. Addition of Device Models to the List

3.1 For SMETS2+ Device Models, the Panel shall only add Device Models to the Central Products List once the Panel has received all the Assurance Certificates required (under the Technical Specifications) to be obtained in respect of Device Models of the relevant Physical Device Type (which Assurance Certificates may be provided to the Panel by a Party or any other person).

3.2 For SMETS1 Device Models, the Panel shall only add a Device Model to the Central Products List once the Panel has received a notification from the DCC or, subject to Clause 3.5, from a Supplier Party. Clauses 3.3 to 3.13 (inclusive) set out the process for adding SMETS1 Device Models to the Central Products List.

3.3 The DCC shall only send a notification to the Panel in respect of a SMETS1 Device Model (as referred to in Clause 3.2) once the Device Model has been included as part of at least one entry on the SMETS1 Eligible Products Combinations list.

3.4 A Supplier Party may only send a notification to the Panel in respect of a SMETS1 Device Model (as referred to in Clause 3.2) if:

(a) that SMETS1 Device Model has not been included as part of at least one entry on the SMETS1 Eligible Product Combinations list; and

(b) that Supplier Party reasonably believes that the addition of the SMETS1 Device Model to the Central Products List is required in order to facilitate the urgent

resolution of a material security vulnerability relating to Commissioned Devices for which it is the Responsible Supplier.

3.5 As soon as reasonably practicable after sending a notification to the Panel in accordance with Clause 3.2, the relevant Supplier Party shall notify the DCC via the Notification Interface that it has sent such a notification to the Panel and, in doing so, shall inform the DCC of the Device Model notified to the Panel.

3.6 The Panel shall only accept and process a notification from a Supplier Party under Clause 3.2 if the notification has been made in accordance with the requirements of the Supplier Party CPL Notification Procedures and where the Panel has successfully confirmed that the notification was from a Supplier Party and has not been modified since its creation.

3.7 For the purposes of Clause 3.6, the Supplier Party CPL Notification Procedures are procedures that provide for a Device Model to be notified to the Panel by a Supplier Party in a manner that allows the Panel to confirm that:

(a) any such notification has originated from a Supplier Party; and

(b) any such notification from a Supplier Party has not been modified since its creation.

3.8 The Panel shall develop the Supplier Party CPL Notification Procedures and any subsequent modification to them in consultation with the Security Sub-Committee and publish the Supplier Party CPL Notification Procedures on the Website.

3.9 Where the DCC has received a notification via the Notification Interface from a Supplier Party pursuant to Clause 3.5, the DCC shall, as soon as reasonably practical after uploading into the DCC Systems a revised version of the Central Products List that additionally includes the Device Model notified to the Panel by the Supplier Party, inform that Supplier Party via the Notification Interface that the upload has taken place.

3.10 For the purposes of Clauses 3.5 and 3.9, the Notification Interface is an appropriately secure interface, the identity of which the DCC shall communicate to Supplier Parties,

for the purposes of making the notifications between Supplier Parties and the DCC referred to in those Clauses.

3.11 After the addition of a Non-EPCL Device Model to the Central Products List, the Supplier Party that notified the Non-EPCL Device Model to the Panel shall take all reasonable steps to ensure that each Device Model Combination:

(a) of which any Commissioned Device of that Non-EPCL Device Model forms part; and

(b) for which Commissioned Device it is the Responsible Supplier,

is added to the SMETS1 Eligible Product Combinations List as soon as reasonably practicable.

3.12 After the Commissioning of a Device that is of a Non-EPCL Device Model, the Responsible Supplier for that Device shall take all reasonable steps to ensure that that the Device Model Combination of which that Device forms part is added to the SMETS1 Eligible Product Combinations List as soon as reasonably practicable.

3.13 Where a PPMID of a particular type is capable of forming part of either a SMETS1 Smart Metering System or a SMETS2+ Smart Metering System, any Device Model added to the Central Products List shall:

(a) insofar as it relates to PPMIDs of that type forming part of SMETS2+ Smart Metering Systems, be the Manufacturer of the PPMID, its model, its hardware version and its firmware version; and

(b) insofar as it relates to PPMIDs of that type forming part of SMETS1 Smart Metering Systems, be the Manufacturer of the PPMID, its model, its hardware version and a value representing its firmware version that is different to the firmware version of the PPMID of that type that forms part of a SMETS2+ Smart Metering System.

4. Association of Hashes with Device Models on the CPL

4.1 Where the DCC, a Supplier Party or a Manufacturer which is a Party wishes the Panel to associate the Hash of a Manufacturer Image with a Device Model on the Central

Products List, that Party shall provide the Hash and the identity of the person who created the Manufacturer Image in a communication to the Panel which has been Digitally Signed by the person who created the Manufacturer Image in a manner that reasonably enables the Panel to check that the communication originates from the person who created the Manufacturer Image.

4.2 The Panel may specify the format which the communication referred to in Clause 4.1 must take (in which case Parties sending such communications must use such format). The Panel shall notify the relevant Parties of any such required format and of any changes to such required format that the Panel may make from time to time.

4.3 The Panel shall only associate a Hash provided under Clause 4.1 with a Device Model on the Central Products List where:

(a) the Panel has successfully confirmed that the Digital Signature referred to in Clause 4.1 is that of the person who created the Manufacturer Image (validated as necessary by reference to a trusted party);

(b) there is no Hash currently associated with the Device Model; provided that, if there is a Hash currently associated with the Device Model, the Panel shall investigate the matter with the relevant Parties to identify whether it is appropriate to replace the associated Hash (and shall, where it is appropriate to do so, update the Central Products List accordingly); and

(c) if the Device Model is a SMETS1 Device Model, the communication to the Panel referred to in Clause 4.1 is from the DCC.

5. Adding Device Models to CPA Certificates

5.1 An existing CPA Certificate for a Device Model may allow one or more additional Device Models to be added under that existing CPA Certificate, provided that any additional Device Model differs from the Device Model for which the CPA Certificate was originally issued only by virtue of having different versions of hardware and/or firmware that do not have a significant impact on the security functions of the Device Model (as set out in the CPA Assurance Maintenance Plan). Where this is the case,

the following persons may notify the Panel of one or more additional Device Models to be added to the CPA Certificate:

(a) the DCC for Communications Hubs; or

(b) a Supplier Party or a Manufacturer ~~which is a~~ Party for Device Models of all other Physical Device Types.

5.2 Where the DCC, a Supplier Party or a Manufacturer ~~which is a~~ Party notifies the Panel of an additional Device Model pursuant to Clause 5.1, the DCC, Supplier Party or Manufacturer Party shall:

(a) only do so in accordance with the terms of the relevant CPA Assurance Maintenance Plan; and

(b) retain evidence that it has acted in accordance with the terms of the relevant CPA Assurance Maintenance Plan, such evidence to be provided to the Panel or the Authority on request.

5.3 The Panel shall not be required to check whether the DCC, a Supplier Party or Manufacturer (as applicable) is entitled to add a Device Model under the terms of the CPA Certificate and the CPA Assurance Maintenance Plan (as described in Clause 5.1).

5.4 [NOT IN USE]

6. Removal of Device Models from the List

6.1 Where an Assurance Certificate for a Device Model which was issued by the ZigBee Alliance or the DLMS User Association is withdrawn or cancelled by the ZigBee Alliance or the DLMS User Association (as applicable), then the Panel shall remove that Device Model from the Central Products List.

6.2 Where a CPA Certificate for a Device Model expires or is not renewed or is withdrawn or cancelled by ~~NCSC~~the CPA Scheme Operator (acting in accordance with the CPA Policies and Procedures) or a Trial Device Certificate for a Trial Device Model expires or is withdrawn or cancelled by the Security Sub-Committee, then the Security Sub-Committee shall determine whether the Device Model is to be removed from the

Central Products List, and the Panel shall remove the Device Model (or not) as determined by the Security Sub-Committee. In reaching such a determination, the Security Sub-Committee:

(a) shall consider the security implications of such circumstances, and weigh them against the consequences for Energy Consumers of Devices of the relevant Device Model being Suspended as a result of removing the Device Model from the Central Products List;

(b) shall take into account any relevant information provided to it by ~~NCSC~~the CPA Scheme Operator concerning the risks associated with the cancellation, withdrawal or expiry without renewal of the CPA Certificate;

(c) may determine, whether or not the Device Model is to be removed from the Central Product List, that a CPA Certificate Remedial Plan or a Trial Device Remedial Plan (as relevant) is to be imposed (for SMETS2+ Communications Hubs) on the DCC or (for all other Device Models) on the Import Suppliers (for Devices of that Device Model forming part of a Smart Metering System for which they are the Import Supplier) and/or the Gas Suppliers (for Devices of that Device Model forming part of a Smart Metering System for which they are the Gas Supplier); and

(d) shall reach a determination as soon as reasonably practicable taking into account the seriousness of the potential security consequences.

6.3 Where the Security Sub-Committee determines under Clause 6.2 that a CPA Certificate Remedial Plan or a Trial Device Remedial Plan (as relevant) is to be imposed on one or more Parties, then the Security Sub-Committee shall notify those Parties and each of those Parties shall:

(a) (within such period as the Security Sub-Committee may require) propose a plan to the Security Sub-Committee setting out how the Party intends to remedy the security issue or issues that have resulted in or arise from the cancellation, withdrawal or expiry without renewal of the CPA Certificate or Trial Device Certificate, and within what time period;

(b) (within such period as the Security Sub-Committee may require) take into account any and all comments on the proposed plan raised by the Security Sub-Committee, and obtain the Security Sub-Committee's approval of the plan (the approved plan for each such Party, as modified from time to time with the approval of the Security Sub-Committee, being that Party's "CPA Certificate Remedial Plan" or, in the case of a Trial Device Certificate, its "Trial Device Remedial Plan");

(c) comply in all material respects with the CPA Certificate Remedial Plan or Trial Device Remedial Plan (as relevant); and

(d) (where requested by the Security Sub-Committee) report to the Security Sub-Committee on progress in respect of the CPA Certificate Remedial Plan or Trial Device Remedial Plan (as relevant).

6.4 Where the Security Sub-Committee initially determines under Clause 6.2 that a CPA Certificate Remedial Plan or Trial Device Remedial Plan (as relevant) is to be imposed as an alternative to removing a Device Model from the Central Products List, then the Security Sub-Committee may at any time determine that the Device Model in question is to be removed from the Central Products List, in which case the Panel shall remove the Device Model from the Central Products List.

6.5 For the purposes of Section M8.1(g) (Events of Default), the obligations of a Party under Clause 6.3 are material obligations. Accordingly, failure by a Party to gain approval for, or failure by a Party to comply in all material respects with, a CPA Certificate Remedial Plan shall be an Event of Default if not remedied within 20 Working Days after notice from the Security Sub-Committee requiring remedy.

6.6 The DCC, each Supplier Party and each Manufacturer ~~which is a~~ Party shall provide such relevant information as the Security Sub-Committee may reasonably request to assist it in reaching a determination under Clause 6.2 or 6.4.

6.7 The DCC, each Supplier Party and each Manufacturer ~~which is a~~ Party shall notify the Panel of any withdrawal, expiry or cancellation of an Assurance Certificate of which the DCC, Supplier Party or Manufacturer Party becomes aware. Where removal occurs as a result of the withdrawal, expiry or cancellation of an Assurance Certificate,

the Panel shall only remove a Device Model from the Central Products List after the Panel has confirmed with the relevant Assurance Certification Body that the Assurance Certificate for that Device Model has expired or has been withdrawn or cancelled (and no new Assurance Certificate has been provided to the Panel under Clause 3).

6.8 The Panel may also remove a SMETS1 Device Model from the Central Products List where either:

(a) the Security Sub Committee advises that the Device Model should be removed from the Central Products List; or

(b) it is determined by the Authority or by the Panel under Section F3 (Panel Dispute Resolution Role) that Devices of the relevant Device Model are not compliant with SMETS1 (either on their own or in combination with Devices of other Device Models listed on the Central Products List).

6.9 The Panel may reinstate to the Central Products List a SMETS1 Device Model that it has removed pursuant to Clause 6.8; provided that the Panel may only reinstate a Device Model that has been removed pursuant to Clause 6.2A(b) where it determines that the issue that gave rise to the removal of the Device Model has been rectified.

6.10 For the purposes of this Code, a Communications Hub Function or a Gas Proxy Function shall be considered to be on (or not on) the Central Products List if the Communications Hub of which it forms part is on (or not on) the Central Products List.

6.11 The Panel may provide for the removal of a Device Model from the Central Products List by marking that Device Model as 'removed'. All references in this Code to the removal of a Device Model from the Central Products List (and similar expressions) shall be interpreted accordingly.

7. Digital Signatures on CPL

7.1 When providing an updated Central Products List (or extract of it) to the DCC, the Panel shall provide a copy of the Central Products List (or of that extract) that is

Digitally Signed so as to reasonably enable the DCC to check that the updates to the Central Product List originate from the Panel.

7.2 The DCC shall, before using and relying upon the Central Products List received by the DCC from the Panel, first confirm that the Digital Signature referred to in Clause 7.1 is that of the Panel (validated as necessary by reference to a trusted party).

7.3 Following receipt by the DCC of an updated Central Products List from the Panel, the DCC shall take all reasonable steps to establish whether the update included the removal of one or more Device Models from the Central Products List. Where the DCC establishes that an update did include the removal of one or more Device Models from the Central Products List, then:

(a) the DCC shall take all reasonable steps to confirm that it was the intention of the Panel to remove such Device Models from the Central Products List; and

(b) where the DCC reasonably believes that it was not the intention of the Panel to remove such Device Models from the Central Products List, the DCC shall notify the Panel that this is the case and (notwithstanding Section F2.9) shall ignore the updated Central Products List.