

## **G SECURITY**

### **G1. SECURITY: GENERAL PROVISIONS**

#### **Interpretation**

G1.1 Sections G2 to G9 shall be interpreted in accordance with the following provisions of this Section G1.

#### **Transitional Period for Updated or Replacement Standards**

G1.2 Section G1.3 applies where:

- (a) the DCC or any User is required, in accordance with any provision of Sections G2 to G9, to ensure that it, or that any of its policies, procedures, systems or processes, complies with:
  - (i) any standard, procedure or guideline issued by a third party; and
  - (ii) any equivalent to that standard, procedure or guideline which updates or replaces it from time to time; and
- (b) the relevant third party issues an equivalent to that standard, procedure or guideline which updates or replaces it.

G1.3 Where this Section G1.3 applies, the obligation on the DCC or User (as the case may be):

- (a) shall be read as an obligation to comply with the updated or replaced standard, procedure or guideline from such date as is determined by the Panel (having considered the advice of the Security Sub-Committee) in respect of that document; and
- (b) prior to that date shall be read as an obligation to comply (at its discretion) with either:
  - (i) the previous version of the standard, procedure or guideline; or
  - (ii) the updated or replaced standard, procedure or guideline.

G1.4 Any date determined by the Panel in accordance with Section G1.3 may be the subject of an appeal by the DCC or any User to the Authority (whose decision shall be final and binding for the purposes of this Code).

#### **Obligations on Users**

G1.5 Obligations which are expressed to be placed on a User shall, where that User performs more than one User Role, be read as applying to it separately in respect of each of its User Roles.

G1.6 For the purposes of Section G1.5, where any Network Party is deemed to have nominated itself as a Registration Data Provider (in accordance with the definition of Registration Data Provider), its role as a Registration Data Provider shall be treated as if it were an additional category of User Role.

## **Exclusion for Export Suppliers and Registered Supplier Agents**

G1.7 Where a User acts in the User Role of 'Export Supplier' or 'Registered Supplier Agent', it is not to be subject to any of the obligations expressed to be placed on Users except for those obligations set out at:

- (a) Sections G3.2 to G3.3 (Unauthorised Activities: Duties to Detect and Respond);
- (b) Sections G3.8 to G3.9 (Management of Vulnerabilities);
- (c) Sections G5.14 to G5.18 (Information Security: Obligations on Users), save that for this purpose the reference:
  - (i) in Section G5.18(b)(i) to "Sections G3 and G4" shall be read as if it were to "Sections G3.2 to G3.3 and G3.8 to G3.9"; and
  - (ii) in Section G5.18(b)(iii) to "Sections G5.19 to G5.24" shall be read as if it were to "Section G5.19(d)";
- (d) Sections G5.25 and G5.26 (Shared Resources); and
- (e) G6 (Anomaly Detection Thresholds: Obligations on the DCC and Users).

## **Disputes**

G1.8 Where, in any dispute between a Party and a User, a question arises as to whether that User has complied with any of its obligations under Sections G3 to G6:

- (a) that question may be referred by either of them to the Panel for its determination; and
- (b) where either of them disagrees with any such determination of the Panel, then it may refer the matter to the Authority in accordance with Section M7 (Dispute Resolution).

G1.9 Section G1.8:

- (a) shall be without prejudice to the provisions of Section M8.2 (Notification of an Event of Default); and
- (b) shall not apply in respect of any other question in dispute between a Party and a User relating to or arising from the question of whether the User has complied with any of its obligations under Sections G3 to G6.

## **SMETS1 Smart Metering Systems**

G1.10 Any reference in Sections G2 to G9 to:

- (a) a SMETS1 SMS shall be treated as being a reference to an Enrolled SMETS1 SMS only;
- (b) a Smart Metering System shall be treated as including a SMETS1 SMS only if it is an Enrolled SMETS1 SMS;
- (c) a Device shall be treated as including a SMETS1 Device only if it forms part of or is ancillary to an Enrolled SMETS1 SMS.

## **The SMETS1 CSP System**

G1.11 Section G1.12 applies to the DCC in respect of those parts of the DCC Total System which:

- (a) comprise those Systems used by any DCC Service Provider in order to support the provision of Communications Services by the DCC in relation to SMETS1 Devices; and
- (b) do not constitute those Systems used by the DCC in its role as a SMETS1 Service Provider or as a DCO that do not also support the provision of Communications Services by the DCC in relation to SMETS2+ Devices,

and, for the purposes of Section G1.12, those parts of the DCC Total System shall be known as the "**SMETS1 CSP System**".

G1.12 Where this Section G1.12 applies, the DCC may comply with its obligations under the provisions listed in Section G1.13 by, in each case, ensuring that the records, processes or procedures described in that provision are, in respect of the SMETS1 CSP System, compliant with:

- (a) the standard specified in that provision; or
- (b) an alternative standard or methodology that reflects Good Industry Practice in respect of the subject matter of the standard specified in that provision, and that is capable of verification as such by the DCC Independent Security Assurance Service Provider in accordance with Section G9.

G1.13 The provisions listed in this Section G1.13 are the provisions at Sections G2.13, G2.18, G2.26, G2.27, G4.6, G5.7, G5.8 and G5.10.

## **CSS Provider Systems**

G1.14 The security obligations applying to the CSS Provider Systems are set out in Section E2.18 (Security Obligations of the CSS Provider); and

G1.15 In Sections G2 to G9:

- (a) other than for the purposes of Section G2.20(a), each and every reference to the DCC Total System shall exclude the CSS Provider Systems; and
- (b) each and every reference to the DCC Systems shall exclude the CSS Provider Systems.

## **G2. SYSTEM SECURITY: OBLIGATIONS ON THE DCC**

### **Unauthorised Activities: Duties to Detect and Respond**

G2.1 The DCC shall take reasonable steps:

- (a) to ensure that the DCC Systems are capable of detecting any unauthorised connection that has been made to them, and any unauthorised attempt to connect to them, by any other System; and
- (b) if the DCC Systems detect such a connection or attempted connection, to ensure that the connection is terminated or the attempted connection prevented (as the case may be).

G2.2 The DCC shall take reasonable steps:

- (a) to ensure that the DCC Total System is capable of detecting any unauthorised software that has been installed or executed on it and any unauthorised attempt to install or execute software on it;
- (b) if the DCC Total System detects 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.

G2.3 The DCC shall:

- (a) take reasonable steps to ensure that:
  - (i) the DCC Total System is capable of identifying any deviation from its 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 the DCC Total System.

G2.4 The DCC shall take reasonable steps to ensure that the DCC Total System:

- (a) is capable of identifying any unauthorised or unnecessary network port, protocol, communication, application or network service;
- (b) causes or permits to be open at any time only those network ports, and allows only those protocols, which are required at that time for the effective operation of that System, and blocks all network ports and protocols which are not so required; and
- (c) causes or permits at any time only the making of such communications and the provision of such applications and network services as are required at that time for the effective operation of that System.

G2.5 The DCC shall take reasonable steps to ensure that each component of the DCC Total System is, at each point in time, enabled only with the functionality that is necessary for it effectively to fulfil its intended role within the DCC Total System at that time.

G2.6 The DCC shall:

- (a) ensure that the DCC Total System records all system activity (including all attempts to access resources, or Data held, on it) in audit logs;
- (b) ensure that the DCC Total System detects any attempt by any person to access resources, or Data held, on it without possessing the authorisation required to do so; and
- (c) take reasonable steps to ensure that the DCC Total System prevents any such attempt at unauthorised access.

G2.7 The DCC shall take reasonable steps to ensure that the DCC Total System is capable of detecting any instance of Data leaving it by any means (including in particular by network transfers and the use of removable media) without authorisation.

## **Adverse Events: Duties to Detect and Prevent**

G2.8 The DCC shall take reasonable steps to ensure that:

- (a) the DCC Total System detects any Denial of Service Event; and
- (b) any unused or disabled component or functionality of the DCC Total System is incapable of being a means by which that System is Compromised.

G2.9 The DCC shall use its best endeavours to:

- (a) ensure that the DCC Total System is not Compromised;
- (b) where the DCC Total System is Compromised, minimise the extent to which it is Compromised and any adverse effect arising from it having been Compromised; and
- (c) ensure that the DCC Total System detects any instance in which it has been Compromised.

## **Security Incident Management**

G2.10 The DCC shall ensure that, where the DCC Total System detects any:

- (a) unauthorised event or deviation of a type referred to in Sections G2.1 to G2.7; or
  - (b) event which results, or was capable of resulting, in the DCC Total System being Compromised,
- the DCC takes all of the steps required by the DCC Information Security Management System.

G2.11 The DCC shall, on the occurrence of a Major Security Incident in relation to the DCC Total System:

- (a) promptly notify the Panel and the Security Sub-Committee (unless paragraph (b) applies); or
- (b) where the Major Security Incident relates to that part of the DCC Total System which consists of any parts of the SMETS1 CSP System in respect of which Telefonica UK Limited is the DCC Service Provider, notify the Panel and the Security Sub-Committee as soon as is reasonably practicable.

## **System Design and Operation**

G2.12 G2.12 The DCC shall, at each stage of the System Development Lifecycle, have regard to the need to design and operate the DCC Total System so as to protect it from being Compromised.

## **Management of Vulnerabilities**

G2.13 The DCC shall ensure that an organisation which is a CHECK approved service provider or a CREST certified tester carries out assessments that are designed to identify any vulnerability of the DCC Systems to Compromise:

- (a) in respect of each DCC System, on at least an annual basis;
- (b) in respect of each new or materially changed component or functionality of the DCC Systems, prior to that component or functionality becoming operational; and

- (c) on the occurrence of any Major Security Incident in relation to the DCC Systems.
- G2.14 The DCC shall ensure that it carries out assessments that are designed to identify any vulnerability of the DCC Systems to Compromise:
- (a) in respect of each DCC System, on at least an annual basis;
  - (b) in respect of each new or materially changed component or functionality of the DCC Systems, prior to that component or functionality becoming operational; and
  - (c) on the occurrence of any Major Security Incident in relation to the DCC Systems.
- G2.15 Where, following any assessment of the DCC Systems in accordance with Section G2.13 or G2.14, any such vulnerability has been detected, the DCC shall:
- (a) take 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; and
  - (b) in the case of a material vulnerability, promptly notify 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.

### **Management of Data**

- G2.16 Where the DCC carries out a Back-Up of any Data held on the DCC Total System, it shall ensure that the Data which are Backed-Up are:
- (a) protected in accordance with the Information Classification Scheme, including when being transmitted for the purposes of Back-Up; and
  - (b) stored on media that are located in physically secure facilities, at least one of which facilities must be in a different location to that part of the DCC Total System on which the Data being Backed-Up is ordinarily held.
- G2.17 The DCC shall develop and maintain, and hold all Data in accordance with, a DCC Data Retention Policy.
- G2.18 The DCC shall ensure that where, in accordance with the DCC Data Retention Policy, any Data are no longer required for the purposes of the Authorised Business, they are securely deleted in compliance with:
- (a) HMG Information Assurance Standard No. 5:2011 (Secure Sanitisation); or
  - (b) any equivalent to that HMG Information Assurance Standard which updates or replaces it from time to time.

### **DCC Total System: Duty to Separate**

- G2.19 The DCC shall take reasonable steps to ensure that any software or firmware installed on the DCC Total System for the purposes of security is Separated from any software or firmware that is installed on that System for any other purpose.
- G2.20 The DCC shall ensure that:

- (a) all DCC Systems which form part of the DCC Total System are Separated from any other Systems;
- (b) the DCC IT Testing and Training Systems and DCC IT Supporting Systems are Separated from the DCC Live Systems; and
- (c) subject to the provisions of Section G2.22, each DCC Individual Live System is Separated from each other such System.

G2.21 Not used.

G2.22 Any System of the type referred to at paragraph (b) of the definition of DCC Individual Live System in Section A1 (Definitions) need not be Separated from that part of the DCC Total System which is used to convey communications between it and SMETS1 CHs.

**DCC Total System: Further provisions for those parts referred to in paragraphs (b) and (c) of the definition of DCC Live Systems**

G2.22A The requirements set out in Section G2.22B apply in relation to:

- (a) the part of the DCC Total System which is referred to in paragraph (b) of the definition of DCC Live Systems in Section A1 (Definitions); and
- (b) the part of the DCC Total System which is referred to in paragraph (c) of the definition of DCC Live Systems in Section A1 (Definitions),

each of which is as a '**relevant system**' for the purposes of Section G2.22B.

G2.22B The DCC shall ensure that:

- (a) where a relevant system receives information from, or purporting to be from, the other relevant system, the relevant system receiving the information shall, prior to that information being used by any person, verify that the information:
  - (i) originated from and was created by the other relevant system; and
  - (ii) has not been modified since it was created by that relevant system;
- (b) it puts in place such additional controls, practices and procedures which (to the extent possible) mitigate the risk of a member of DCC Personnel or a member of personnel of any DCC Service Provider being able to introduce or cause a security vulnerability in a relevant system;
- (c) any person engaged in the development or customisation of any bespoke firmware or software relating to a relevant system is not, including for a period of at least 24 months (or such shorter period as may be approved by the Security Sub-Committee) following the date on which they cease to be so engaged on that relevant system, engaged in the development or customisation of bespoke firmware or software relating to the other relevant system;
- (d) any person that is authorised as a Privileged Person in relation to a relevant system is not, including for a period of a least six months following the date on which they cease to be authorised as such a Privileged Person for that relevant system, authorised as a Privileged Person in relation to the other relevant system;

- (e) any person that is a DCC Service Provider in respect of a relevant system is not a DCC Service Provider in respect of the other relevant system nor an Affiliate or Related Undertaking of any such DCC Service Provider; and
- (f) any independent security testing of a relevant system that is used to provide assurance must be carried out by an organisation which is a CHECK approved service provider or a CREST certified tester but is not an organisation that:
  - (i) designed or developed any relevant system; or
  - (ii) is an Affiliate or Related Undertaking of an organisation that has designed or developed any relevant system.

**DCC Total System: Further provisions for that part referred to in paragraph (c) of the definition of DCC Live Systems**

- G2.22C The requirements in Sections G2.22D and G2.22E apply in relation to the part of the DCC Total System referred to in paragraph (c) of the definition of DCC Live Systems and referred to in Sections G2.22D and G2.22E the 'applicable system').
- G2.22D The DCC shall ensure that each DCC Service Provider in respect of the applicable system shall, as soon as reasonably practicable, procure, from each company or other person that it knows or should reasonably know is at any time an Ultimate Controller of the DCC Service Provider, a legally enforceable undertaking in favour of the DCC the terms of which provide that the Ultimate Controller will refrain from any action that would be likely to cause the DCC Service Provider to be unable to meet the requirements imposed on it by the DCC for the purposes of enabling the DCC to comply with Section G2.22B(e).
- G2.22E The DCC shall ensure that each DCC Service Provider Contract in respect of Services relating to the applicable system shall include terms and conditions which:
- (a) require the DCC Service Provider to ensure that it is at all times able to meet the requirements imposed on it by the DCC for the purposes of enabling the DCC to comply with Section G2.22B(e);
  - (b) provide that where the DCC Service Provider:
    - (i) fails to procure an undertaking required by the DCC under Section G2.22C; or
    - (ii) fails to meet the requirements imposed on it by the DCC for the purposes of enabling the DCC to comply with Section G2.22B(e),
 the DCC shall be entitled under and in accordance with the DCC Service Provider Contract to:
    - (iii) require such divestment by the DCC Service Provider as will enable it to meet the requirements imposed on it by the DCC for the purposes of its compliance with Section G2.22B(e);
    - (iv) terminate the DCC Service Provider Contract in respect of the applicable system and recover from the DCC Service Provider the DCC's costs arising as a direct result of the DCC Service Provider's failure as referred to in Sections G2.22E(b)(i) and (ii), including any fines or re-procurement costs.



## **Transfer of Secret Key Material**

- G2.22F Section G2.22G applies where the services provided under any particular DCC Service Provider Contract are (or are to be) replaced (in whole or in part) by the DCC such that they are (or shall be) provided under a different DCC Service Provider Contract.
- G2.22G Where this Section G2.22G applies and it is expedient or requisite for the purposes of enabling the DCC to ensure the secure, continued and ongoing provision of services provided by the DCC under the Smart Energy Code, the DCC may, subject to the requirements of Section G2.22I, securely transfer Secret Key Material and other associated information from one DCC Live System or DCC Individual Live System to another DCC Live System or DCC Individual Live System or to a system which is to become part of a DCC Live System or DCC Individual Live System.
- G2.22H Where:
- (a) a secure transfer of Secret Key Material takes place pursuant to the provisions of Section G2.22G; and
  - (b) the transferred Secret Key Material includes a Private Key,
- any Certificate that contains a Public Key that is associated with that Private Key shall, for the purposes of the Code, be treated as having been issued in respect of the DCC Live System or DCC Individual Live System to which that Secret Key Material has been transferred.
- G2.22I The requirements of this Section G2.22I are that where the Secret Key Material relates to, or is used in connection with any Public Key that is the subject of, this Code:
- (a) the SMKI PMA has, prior to the transfer of the Secret Key Material or other associated information taking place and having taken account of the views of the Security Sub-Committee on the proposed transfer, approved both:
    - (i) the secure transfer of that Secret Key Material and any other associated information; and
    - (ii) the secure mechanism by which the transfer is to take place; and
  - (b) the DCC ensures that:
    - (i) the secure transfer of the Secret Key Material and any other associated information is undertaken in compliance with any conditions that maybe specified by the SMKI PMA in its approval (which approval may be given before this Section G2.22I takes effect); and
    - (ii) the system to which the Secret Key Material and any other associated information is transferred complies with the requirements of Section G, including where that system is to become part of a DCC Live System or a DCC Individual Live System that it complies (to the extent required) with the provisions of Section G that apply or will apply to that DCC Live System or DCC Individual Live System.

## **DCC Live Systems: Independence of User Systems**

- G2.23 The DCC 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 the DCC Live Systems; or
- (b) the development, design, build, testing, configuration, implementation, operation, maintenance, modification or decommissioning of any part of the DCC Live Systems,

unless that individual satisfies the requirements of Section G2.24.

G2.24 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 G2.23, 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 User Systems; or
  - (ii) the development, design, build, testing, configuration, implementation, operation, maintenance, modification or decommissioning of any User Systems; and
- (b) has not been engaged in any activity described in paragraph (a) for a period of time which the DCC reasonably considers to be appropriate, having regard to the need to ensure the management of risk in accordance with the DCC Information Security Management System.

G2.25 The DCC shall ensure that no resources which form part of the DCC Live Systems also form part of any User Systems.

### **Monitoring and Audit**

G2.26 The DCC shall ensure that all system activity audit logs are reviewed regularly in accordance with the DCC Information Security Management System.

G2.27 The DCC shall ensure that all such system activity recorded in audit logs is recorded in a standard format which is compliant with:

- (a) British Standard BS 10008:2008 (Evidential Weight and Legal Admissibility of Electronic Information), or any equivalent to that British Standard which updates or replaces it from time to time; and
- (b) in the case of activity on the DCC Systems only, the Security Sub-Committee Guidance on Forensic Readiness published on the Website.

G2.28 The DCC shall monitor the DCC Systems in compliance with the SMKI PMA Guidance on Protective Monitoring published on the Website.

G2.29 The DCC shall take reasonable steps to ensure that the DCC 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, Commands, Instructions to SMETS1 Devices, Service Responses and Alerts;
- (b) audit logs of each component of the DCC Total System;

- (c) error messages generated by each device which forms part of the DCC Total System;
- (d) Incident Management Log compiled in accordance with Section H9; and
- (e) patterns of traffic over the SMETS1 SM WAN and the SMETS2+ SM WAN.

G2.30 The DCC shall:

- (a) take reasonable steps to ensure that the DCC Systems detect all Anomalous Events; and
- (b) ensure that, on the detection of any Anomalous Event, it takes all of the steps required by the DCC Information Security Management System.

### **Manufacturers: Duty to Notify and Be Notified**

G2.31 Where the DCC becomes aware of any material security vulnerability in, or likely cause of a material adverse effect on the security of, any hardware, software or firmware which forms part of the DCC Total System, it shall:

- (a) wherever it is reasonably practicable to do so notify the manufacturer of the hardware 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) promptly notify the Security Sub-Committee 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.

G2.32 The DCC shall not be required to notify a manufacturer or developer in accordance with Section G2.31(a) where it has reason to be satisfied that the manufacturer or developer is already aware of the matter that would otherwise be notified.

G2.33 The DCC shall, wherever it is reasonably practicable to do so, establish with the manufacturers of the hardware and developers of the software and firmware which form part of the DCC Total System arrangements designed to ensure that the DCC 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 or firmware.

G2.34 Any arrangements established in accordance with Section G2.33 may provide that the manufacturer or developer (as the case may be) need not be required to notify the DCC where that manufacturer or developer has reason to be satisfied that the DCC is already aware of the matter that would otherwise be notified under the arrangements.

### **Parse and Correlate Software: Duty to Notify**

G2.35 Where the DCC becomes aware of any material security vulnerability in, or likely cause of a material adverse effect on the security of, any version of the Parse and Correlate Software, it shall notify the Users and (wherever it is reasonably practicable to do so) the developer of the software.

- G2.36 The DCC shall not be required to notify a developer or User in accordance with Section G2.35 where it has reason to be satisfied that the developer or User is already aware of the matter that would otherwise be notified.

### **Cryptographic Credential Tokens and Smart Card Tokens**

- G2.37 Before supplying any Cryptographic Credential Token or Smart Card Token to any person in accordance with the provisions of this Code, the DCC shall ensure that the version of the software which forms part of that Cryptographic Credential Token or Smart Card Token:
- (a) operates so as to generate Public Keys each of which is part of a Key Pair that has been generated using random numbers which are such as to make it computationally infeasible to regenerate that Key Pair even with knowledge of when and by means of what equipment it was generated; and
  - (b) has been adequately tested for the purpose of ensuring that it fulfils its intended purpose.
- G2.38 The DCC shall, wherever it is reasonably practicable to do so, establish with the manufacturers of the hardware and developers of the software and firmware which form part of any Cryptographic Credential Tokens or Smart Card Tokens to be supplied by it in accordance with the provisions of this Code, arrangements designed to ensure that the DCC 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 or firmware.
- G2.39 Where the DCC becomes aware of any material security vulnerability in, or likely cause of a material adverse effect on the security of, any hardware, software or firmware which form part of any Cryptographic Credential Token or Smart Card Token which has been supplied by it in accordance with the provisions of this Code, it shall notify the Subscribers for Certificates associated with the use of Cryptographic Credential Tokens or Smart Card Tokens and (wherever it is reasonably practicable to do so) the manufacturer of the hardware or (as the case may be) developer of the software or firmware.

### **File Signing Software**

- G2.40 Before supplying any File Signing Software to any person in accordance with the provisions of this Code, the DCC shall ensure that the version of that File Signing Software which is being supplied has been subject to a software code review, by an individual or organisation with the professional competence to carry out such a review, for the purpose of identifying any vulnerabilities in the code that were not intended as a feature of its design.
- G2.41 The DCC shall, wherever it is reasonably practicable to do so, establish with the developer of the File Signing Software to be supplied by it in accordance with the provisions of this Code, arrangements designed to ensure that the DCC will be notified where that developer becomes aware of any material security vulnerability in, or likely cause of a material adverse effect on the security of, such software.
- G2.42 Where the DCC becomes aware of any material security vulnerability in, or likely cause of a material adverse effect on the security of, any File Signing Software which has been supplied by it in accordance with the provisions of this Code, it shall notify each person to whom it has provided that software and (wherever it is reasonably practicable to do so) the developer of the software.
- G2.43 The DCC shall ensure that where it provides File Signing Software to any person, that software is provided in a format such that it can be confirmed, on receipt by the person to whom it is provided, as:

- (a) having been provided by the DCC; and
- (b) being authentic, such that any tampering with the software would be apparent.

### **Cryptographic Processing**

G2.44 The DCC shall ensure that all Cryptographic Processing which:

- (a) is for the purposes of complying with its obligations as CoS Party;
- (b) results in the application of a Message Authentication Code to any message in order to create a Command to be sent to a SMETS2+ Device;
- (c) is carried out by a DCO and involves the use for a SMETS1 Symmetric Key;
- (d) involves the use of a DCC Private Key to establish any Transport Layer Security for the purposes of communicating with a SMETS1 Device;
- (e) (other than in any of the circumstances set out in Section G2.44A) is carried out by a SMETS1 Service Provider and involves the use of a SMETS1 Symmetric Key; or
- (f) (other than in any of the circumstances set out in Section G2.44B) involves the use of a Private Key to create a Digital Signature which is intended to be part of a Command that can be processed by a SMETS2+ Device,

is carried out within Cryptographic Modules which are compliant with FIPS 140-2 Level 3 (or any equivalent to that Federal Information Processing Standard which updates or replaces it from time to time).

G2.44A For the purposes of Section G2.44(e), the circumstances set out in this Section G2.44A shall be those in which one of the following occurs:

- (a) Cryptographic Processing is carried out by a SMETS1 Service Provider to generate a Command to "add credit" (as specified in a Version of the ESMETS, the GSMETS or the IHDTs with a Principal Version number of 1) to a SMETS1 Device;
- (b) a SMETS1 Symmetric Key is used by a SMETS1 Service Provider to generate an Instruction where the target Device is identified in the SMETS1 Supporting Requirements as a Category 1 Device for the purposes of this paragraph (b);
- (c) a SMETS1 Symmetric Key is used by a SMETS1 Service Provider where:
  - (i) that Symmetric Key is valid only for the duration of a single Application Association; and
  - (ii) the target Device is identified as a Category 2 Device for the purposes of this sub-paragraph in the SMETS1 Supporting Requirements; and
- (d) any use of a SMETS1 Symmetric Key by a SMETS1 Service Provider that is:
  - (i) required to establish a session for Transport Layer Security with a SMETS1 Device;
  - (ii) generated as part of the establishment of the session; and

- (iii) destroyed at the termination of that same session.

G2.44B For the purposes of Section G2.44(f), the circumstances set out in this Section G2.44B shall be where:

- (a) in relation to a Recovery Private Key, there is a period of time during which that Recovery Private Key is unusable for the purposes set out in G2.44 because of it being split into multiple parts as described in Appendix L (SMKI Recovery Procedure); and
- (b) in relation to the Contingency Private Key, there is a period of time during which the Contingency Private Key is unusable for the purposes set out in G2.44 because of it being split into multiple parts as described in Appendix L (SMKI Recovery Procedure).

G2.45 The DCC shall ensure that any and all Cryptographic Processing undertaken under or pursuant to this Code which does not fall within the scope of Section G2.44 is carried out within Cryptographic Modules established in accordance with its Information Classification Scheme.

### **Network Time**

G2.46 For the purposes of Section G2.47:

- (a) the "**Network Time**" means one or more time sources maintained by the DCC from which all Commissioned Communications Hub Functions synchronise time; and
- (b) the "**Independent Time Source**" means a time source that is:
  - (i) accurate;
  - (ii) not maintained by the DCC; and
  - (iii) determined in a manner that is independent of any part of the DCC Total System.

G2.47 The DCC shall ensure that:

- (a) the DCC Total System is capable of detecting any instance in which the Network Time materially differs from the Independent Time Source; and
- (b) if the DCC Total System detects such a material difference, the DCC takes all of the steps required by the DCC Information Security Management System to rectify the inaccuracy of its Network Time.

### **Integrity of Communication over the SM WAN**

G2.48 The DCC shall take reasonable steps to ensure that all communications which are transmitted over the SM WAN are protected so that the Data contained in them remains confidential, and their integrity is preserved, at all times during transmission to and from Communications Hubs.

G2.49 The DCC shall not process any communication received over the SM WAN, or send to any Party any communication over the SM WAN, where it is aware that the Data contained in that communication has been Compromised.

## ECoS Interface Specification

- G2.50 The DCC shall, as soon as reasonably practicable after the coming into effect of this Section G2.50, prepare and submit to the Secretary of State for approval an ECoS Interface Specification in accordance with the following process:
- (a) the DCC shall send a draft of the ECoS Interface Specification, together with an impact assessment that sets out the DCC's views on any impact that the subject matter of the draft ECoS Interface Specification might reasonably be considered to have on the End-to-End Security Architecture or the risks identified in the Security Risk Assessment (a **Security Impact Assessment**), to the Security Sub-Committee for its review and comments;
  - (b) having received the Security Sub-Committee's comments and observations on the Security Impact Assessment, the DCC shall as soon as is practicable provide a response to any such comments or observations to the Security Sub-Committee, update the draft ECoS Interface Specification as appropriate to take into account any such comments and observations, and send the updated draft to the Secretary of State, together with:
    - (i) a statement of the reasons why the DCC considers the submitted draft to be fit for purpose; and
    - (ii) an explanation of how the DCC has responded to the comments and observations (if any) made by the Security Sub-Committee in respect of the initial draft and/or the Security Impact Assessment sent to it in accordance with paragraph (a) above;
  - (c) the DCC shall comply with any direction given to it by the Secretary of State following the Secretary of State's consideration of the draft ECoS Interface Specification which direction may require the DCC to:
    - (i) make such amendments to the draft document as are set out or described in the direction;
    - (ii) produce and submit to the Secretary of State a further draft of the document; and
    - (iii) follow a specified process (and the time within which that process shall be completed) prior to submitting a further draft of the document to the Secretary of State.
- G2.51 Where pursuant to Section G2.50(b) the Security Sub-Committee receives a response from the DCC in respect of any comments or observations made by the Security Sub-Committee on the Security Impact Assessment, the Security Sub-Committee shall notify the Secretary of State whether it considers there to be any remaining outstanding unacceptable risks to the End-to-End Security Architecture as a consequence of the proposed ECoS Interface Specification.
- G2.52 [Not used]
- G2.53 Where the DCC wishes to make a change to the ECoS Interface Specification, it shall prepare and submit to the Security Sub-Committee a draft of the proposed amended ECoS Interface Specification, together with an updated Security Impact Assessment that sets out the DCC's views on the impact that the proposed changes might reasonably be considered to have on the End-to-End Security Architecture or the risks identified in the Security Risk Assessment.

G2.54 The DCC shall take into account, and provide a response to, any comments and observations received from the Security Sub Committee when finalising any replacement version of the ECoS Interface Specification.

G2.55 The DCC shall ensure that:

- (a) the ECoS Interface Specification accurately describes the ECoS Interface at all times; and
- (b) on receiving a request from the DCC Independent Security Assessment Service Provider for the purposes of enabling it to carry out a DCC Security Assessment, the ECoS Interface Specification is made available to the DCC Independent Security Assessment Service Provider together with all previous versions of the specification and any supporting Security Impact Assessments as may be requested by the DCC Independent Security Assessment Service Provider.

### **DCC Use of Private Keys**

G2.56 The DCC 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.

G2.57 Where:

- (a) the DCC is the Subscriber for an Organisation Certificate that has a Remote Party Role that is specified in the GB Companion Specification; and
- (b) the Private Key associated with the Public Key contained within that Organisation Certificate is used for purposes that are not specified or described in the GB Companion Specification,

the DCC shall, where reasonably possible at the earliest opportunity but in any event no later than the date of expiry of that Organisation Certificate, replace the Private Key with one that has an associated Public Key that is contained within an Organisation Certificate that has a Remote Party Role that is specified in Table 1 to Annex A of Section L.

G2.58 Subject to Section G2.59, the DCC shall not, on or from a date which is after the ECoS Service Live Date, become a Subscriber for an Organisation Certificate that:

- (a) has a Remote Party Role that is specified in the GB Companion Specification; and
- (b) contains a Public Key which has an associated Private Key that is used, or is to be used, for purposes that are not specified or described in the GB Companion Specification.

G2.59 The requirement in Section G2.58 shall not apply in circumstances where the DCC is required to replace an Organisation Certificate that has:

- (a) a Remote Party Role that is specified in the GB Companion Specification; and
- (b) been revoked following the operation of one of the procedures in the SMKI Recovery Procedure.

G2.60 The DCC shall ensure that any Root OCA Private Key is used only for the purposes of:



- (a) Digitally Signing an OCA Certificate;
- (b) Digitally Signing a Certificate Signing Request; or
- (c) Digitally Signing the Organisation ARL.

G2.61 The DCC shall ensure that any Issuing OCA Private Key is used only for the purposes of:

- (a) Digitally Signing an Organisation Certificate;
- (b) Digitally Signing a Certificate Signing Request; or
- (c) Digitally Signing the Organisation CRL.

### **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
  - (c) 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.

### **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.

## **G4. ORGANISATIONAL SECURITY: OBLIGATIONS ON USERS AND THE DCC**

### **Obligations on Users**

G4.1 Each User shall:

- (a) ensure that each member of its User Personnel who is authorised to access Data held on its User Systems holds a security clearance which is appropriate to the role performed by that individual and to the Data which he or she is authorised to access; and
  - (b) annually review the security clearance held by each such individual and ensure that it continues to be appropriate to the role performed by that individual and to the Data which he or she is authorised to access.
- G4.2 Each User shall comply with Section G4.3 in respect of any of its User Personnel who are authorised to carry out activities which:
- (a) involve access to resources, or Data held, on its User Systems; and
  - (b) are capable of Compromising the DCC Total System, any User Systems, any RDP Systems or any Device in a manner that could affect (either directly or indirectly) the quantity of gas or electricity that is supplied to a consumer at premises.
- G4.3 Each User shall ensure that any of its User Personnel who are authorised to carry out the activities identified in Section G4.2:
- (a) where they are located in the United Kingdom are subject to security screening in a manner that is compliant with:
    - (i) British Standard BS 7858:2012 (Security Screening of Individuals Employed in a Security Environment – Code of Practice); or
    - (ii) any equivalent to that British Standard which updates or replaces it from time to time; and
  - (b) where they are not located in the United Kingdom are subject to security screening in a manner that is compliant with:
    - (i) the British Standard referred to in Section G4.3(a); or
    - (ii) any comparable national standard applying in the jurisdiction in which they are located.

### **Obligations on the DCC**

- G4.4 The DCC shall:
- (a) ensure that each member of DCC Personnel who is authorised to access Data held on the DCC Total System holds a security clearance which is appropriate to the role performed by that individual and to the Data to which he or she is authorised to access; and
  - (b) annually review the security clearance held by each such individual and ensure that it continues to be appropriate to the role performed by that individual and to the Data to which he or she is authorised to access.
- G4.5 The DCC shall comply with Section G4.6 in respect of any of the DCC Personnel who are authorised to carry out activities which:
- (a) involve access to resources, or Data held, on the DCC Total System; and

- (b) are capable of Compromising the DCC Total System, any User Systems, any RDP Systems or any Device.
- G4.6 The DCC shall ensure that any of the DCC Personnel who are authorised to carry out the activities identified in Section G4.5:
- (a) where they are located in the United Kingdom are subject to security screening in a manner that is compliant with:
    - (i) British Standard BS 7858:2012 (Security Screening of Individuals Employed in a Security Environment – Code of Practice); or
    - (ii) any equivalent to that British Standard which updates or replaces it from time to time; and
  - (b) where they are not located in the United Kingdom are subject to security screening in a manner that is compliant with:
    - (i) the British Standard referred to in Section G4.6(a); or
    - (ii) any comparable national standard applying in the jurisdiction in which they are located.
- G4.7 The DCC shall ensure that each member of DCC Personnel who is a Privileged Person has passed a Security Check before being given any access to Data held on the DCC Total System.
- G4.8 Where the DCC is required to ensure that any two Systems forming part of the DCC Total System are Separated, it shall either:
- (a) ensure that no person is a Privileged Person in relation to both of those Systems; or
  - (b) to the extent that any person is a Privileged Person in relation to both Systems, it establishes additional controls sufficient to ensure that the activities of that person cannot become a means by which any part of the DCC Live Systems is Compromised to a material extent.

## **G5. INFORMATION SECURITY: OBLIGATIONS ON THE DCC AND USERS**

### **Information Security: Obligations on the DCC**

- G5.1 The DCC shall establish, maintain and implement processes for the identification and management of the risk of Compromise to the DCC Total System, and such processes shall comply with:
- (a) the standard of the International Organisation for Standards in respect of information security risk management known as ISO/IEC 27005:2011 (Information Technology – Security Techniques – Information Security Risk Management); or
  - (b) any equivalent to that standard of the International Organisation for Standards which updates or replaces it from time to time
- G5.2 The DCC shall carry out an assessment of such processes for the identification and management of risk:
- (a) on at least an annual basis;
  - (b) on any occasion on which it implements a material change to the DCC Total System; and



- (c) on the occurrence of any Major Security Incident in relation to the DCC Total System.

G5.3 Where the DCC is required in accordance with the DCC Licence to obtain and hold ISO 27001 certification, it shall:

- (a) establish, give effect to, maintain, and comply with a set of policies and procedures to be known as the DCC Information Security Management System;
- (b) ensure that the DCC Information Security Management System:
  - (i) is so designed as to ensure that the DCC complies with its obligations under Sections G2 and G4;
  - (ii) meets the requirements of Sections G5.4 to G5.13; and
  - (iii) provides for security controls which are proportionate to the potential impact of each part of the DCC Total System being Compromised, as determined by means of processes for the management of information risk; and
- (c) review the DCC Information Security Management System on at least an annual basis, and make any changes to it following such a review in order to ensure that it remains fit for purpose.

#### The DCC Information Security Management System

G5.4 The DCC Information Security Management System shall incorporate an information security policy which makes appropriate provision in respect of:

- (a) measures to identify and mitigate risks to the security of Data stored on or communicated by means of the DCC Total System, including measures relating to Data handling, retention and protection; and
- (b) the establishment and maintenance of an Information Classification Scheme in relation to the DCC Total System.

G5.5 The DCC Information Security Management System shall specify the approach of the DCC to:

- (a) information security, including its arrangements to review that approach at planned intervals;
- (b) human resources security;
- (c) physical and environmental security; and
- (d) ensuring that the DCC Service Providers establish and maintain information, human resources, and physical and environmental security measures which are equivalent to those of the DCC.

G5.6 The DCC Information Security Management System shall incorporate a set of asset management procedures which shall make provision for the DCC to establish and maintain a register of the physical and information assets on which it relies for the purposes of the Authorised Business (including a record of the member of DCC Personnel who has responsibility for each such asset).

G5.7 The DCC Information Security Management System shall incorporate procedures that comply with:

- (a) 2021 Telecommunications (Security) Act (TSA) in respect of the security of telecommunications systems and services; or
  - (b) any equivalent to those Security Procedures which update or replace them from time to time.
- G5.8 The DCC Information Security Management System shall incorporate procedures that comply with:
- (a) the appropriate standards of the International Organisation for Standards with respect to network security, comprising ISO/IEC 27033-1:2009, ISO/IEC 27033-2:2012 and ISO/IEC 27033-3:2010 (Information Technology – Security Techniques – Network Security); or
  - (b) any equivalents to those standards of the International Organisation for Standards which update or replace them from time to time.
- G5.9 The DCC Information Security Management System shall incorporate a policy on access control, which includes provision in respect of:
- (a) measures to restrict access to Data that is stored on or communicated by means of the DCC Total System to those who require such Data and are authorised to obtain it;
  - (b) the designation of appropriate levels of identity assurance in respect of those who are authorised to access such Data;
  - (c) the specification of appropriate levels of security clearance in respect of those who are authorised to access such Data;
  - (d) procedures for granting, amending and removing authorisations in respect of access to such Data;
  - (e) procedures for granting and reviewing security clearances for DCC Personnel; and
  - (f) measures to ensure that the activities of one individual may not become a means by which the DCC Total System is Compromised to a material extent.
- G5.10 The DCC Information Security Management System shall incorporate procedures on the management of information security incidents which comply with:
- (a) the standard of the International Organisation for Standards in respect of security incident management known as ISO/IEC 27035:2011 (Information Technology – Security Techniques – Information Security Incident Management); or
  - (b) any equivalent to that standard of the International Organisation for Standards which updates or replaces it from time to time.
- G5.11 The DCC Information Security Management System shall incorporate procedures on the management of information security incidents which in particular make provision for:
- (a) the allocation of clearly defined roles and responsibilities to DCC Personnel;
  - (b) the manner in which such incidents will be monitored, classified, reported and managed;
  - (c) a communications plan in relation to all communications with respect to such incidents; and

- (d) the use of recovery systems in the case of serious incidents.

G5.12 The DCC Information Security Management System shall incorporate procedures on the management of business continuity that comply with:

- (a) the following standards of the International Organisation for Standards in respect of business continuity:
  - (i) ISO/IEC 22301:2012 (Societal Security – Business Continuity Management Systems – Requirements); and
  - (ii) ISO/IEC 27031:2011 (Information Technology – Security Techniques – Guidelines for Information and Communications Technology Readiness for Business Continuity); and
- (b) the Business Continuity Institute Good Practice Guidelines 2013; or
- (c) in each case, any equivalents to those standards or guidelines which update or replace them from time to time.

G5.13 The DCC Information Security Management System shall incorporate procedures in relation to the secure management of all Secret Key Material of the DCC, which shall in particular make provision for:

- (a) the security of that Secret Key Material throughout the whole of its lifecycle from its generation to its destruction;
- (b) the manner in which that Secret Key Material will be registered, ordered, generated, labelled, distributed, installed, superseded and renewed; and
- (c) the verifiable destruction of that Secret Key Material.

#### **Information Security: Obligations on Users**

G5.14 Each User shall establish, maintain and implement processes for the identification and management of the risk of Compromise to:

- (a) its User Systems;
- (b) any security functionality used for the purposes of complying with the requirements of this Section G in relation to its User Systems;
- (c) any other Data, Systems or processes on which it relies for the generation, initiation or processing of Service Requests, Service Responses, Alerts or Data communicated over the Self-Service Interface;
- (d) any Smart Metering Systems for which it is the Responsible Supplier; and
- (e) any communications links established between any of its Systems and the DCC Total System, and any security functionality used in respect of those communications links or the communications made over them.

G5.15 Each User shall ensure that such processes for the identification and management of risk comply with:

- (a) the standard of the International Organisation for Standards in respect of information security risk management known as ISO/IEC 27005:2011 (Information Technology – Security Techniques – Information Security Risk Management); or
- (b) any equivalent to that standard of the International Organisation for Standards which updates or replaces it from time to time.

G5.16 Each User shall carry out an assessment of such processes for the identification and management of risk:

- (a) on at least an annual basis;
- (b) on any occasion on which it implements a material change to:
  - (i) its User Systems;
  - (ii) any security functionality used for the purposes of complying with the requirements of this Section G in relation to its User Systems;
  - (iii) any other Systems or processes on which it relies for the generation, initiation or processing of Service Requests, Service Responses, Alerts or Data communicated over the Self-Service Interface; or
  - (iv) any Smart Metering Systems for which it is the Responsible Supplier; and
- (c) on the occurrence of any Major Security Incident in relation to its User Systems.

G5.17 Each User shall comply with the following standard of the International Organisation for Standards in respect of the security, reliability and resilience of its information assets and processes and its User Systems:

- (a) ISO/IEC 27001:2013 (Information Technology – Security Techniques – Information Security Management Systems); or
- (b) any equivalent to that standard which updates or replaces it from time to time.

G5.18 Each User shall:

- (a) establish, give effect to, maintain, and comply with a set of policies and procedures to be known as its User Information Security Management System;
- (b) ensure that its User Information Security Management System:
  - (i) is so designed as to ensure that it complies with its obligations under Sections G3 and G4;
  - (ii) is compliant with the standard referred to at Section G5.17;
  - (iii) meets the requirements of Sections G5.19 to G5.24; and
  - (iv) provides for security controls which are proportionate to the potential impact of each part of its User Systems being Compromised, as determined by means of processes for the management of information risk; and

- (c) review its User Information Security Management System on at least an annual basis, and make any changes to it following such a review in order to ensure that it remains fit for purpose.

#### The User Information Security Management System

- G5.19 Each User Information Security Management System shall incorporate an information security policy which makes appropriate provision in respect of:
- (a) measures to identify and mitigate risks to the security of Data stored on or communicated by means of the User Systems, including measures relating to Data handling, retention and protection;
  - (b) the establishment and maintenance of an Information Classification Scheme in relation to the User Systems;
  - (c) the management of business continuity; and
  - (d) the education, training and awareness of User Personnel in relation to information security.
- G5.20 Each User Information Security Management System shall specify the approach of the User to:
- (a) information security, including its arrangements to review that approach at planned intervals;
  - (b) human resources security;
  - (c) physical and environmental security; and
  - (d) ensuring that any person who provides services to the User for the purpose of ensuring that the User is able to comply with its obligations under this Code must establish and maintain information, human resources, and physical and environmental security measures which are equivalent to those of the User.
- G5.21 Each User Information Security Management System shall incorporate a set of asset management procedures which shall make provision for the User to establish and maintain a register of the physical and information assets on which it relies for the purposes of complying with its obligations under this Code.
- G5.22 Each User Information Security Management System shall incorporate a policy on access control, which includes provision in respect of:
- (a) measures to restrict access to Data that is stored on or communicated by means of the User Systems to those who require such Data and are authorised to obtain it;
  - (b) procedures for granting, amending and removing authorisations in respect of access to such Data; and
  - (c) measures to ensure that the activities of one individual may not become a means by which the User Systems are Compromised to a material extent.
- G5.23 Each User Information Security Management System shall incorporate procedures on the management of information security incidents which comply with:

- (a) the standard of the International Organisation for Standards in respect of security incident management known as ISO/IEC 27035:2011 (Information Technology – Security Techniques – Information Security Incident Management); or
- (b) any equivalent to that standard of the International Organisation for Standards which updates or replaces it from time to time.

G5.24 Each User Information Security Management System shall incorporate procedures in relation to the secure management of all Secret Key Material of the User, which shall in particular make provision for:

- (a) the security of that Secret Key Material throughout the whole of its lifecycle from its generation to its destruction;
- (b) the manner in which that Secret Key Material will be registered, ordered, generated, labelled, distributed, installed, superseded and renewed; and
- (c) the verifiable destruction of that Secret Key Material.

#### Shared Resources

G5.25 Sections G5.26 to G5.28 apply in relation to a User where:

- (a) any resources which form part of the User Systems of that User (are **Shared Resources**); and
- (b) by virtue of those Shared Resources:
  - (i) the User Systems of that User are capable of being a means by which the User Systems of another User are Compromised (or vice versa); or
  - (ii) the potential extent to which the User Systems of either User may be Compromised, or the potential adverse effect of any Compromise to the User Systems of either User, is greater than it would have been had those User Systems not employed the Shared Resources.

G5.26 Where this Section applies, a User which begins to employ User Systems which consist in whole or in part of Shared Resources:

- (a) shall notify the Security Sub-Committee as soon as reasonably practicable after first doing so; and
- (b) where those Shared Resources are provided to the User by a Shared Resource Provider, shall include in that notification:
  - (i) the name and contact details of the Shared Resource Provider; and
  - (ii) a description of the services provided by the Shared Resource Provider to the User in relation to its User Systems.

G5.27 Where this Section applies, and where a User is entitled to send Critical Service Requests to the DCC, the User shall notify the Security Sub-Committee of the total number of Smart Metering Systems comprising Devices in respect of which such Critical Service Requests are capable of being sent from its User Systems:

- (a) as soon as reasonably practicable after it first begins to employ User Systems which consist in whole or in part of Shared Resources; and
- (b) at intervals of six months thereafter.

G5.28 Where this Section applies:

- (a) the requirement at Section G5.18(b)(iv) shall be read as a requirement on a User to ensure that its User Information Security Management System provides for security controls that are proportionate to the potential impact of a Compromise to each part of all of the User Systems of each User which employs the Shared Resources; and
- (b) where the Shared Resources are provided to a User by a Shared Resource Provider:
  - (i) the provisions of paragraph (a) apply to the Shared Resource Provider in respect of its own User Information Security Management System in the same manner as they apply to each User to which the Shared Resources are provided; and
  - (ii) both the User and the Shared Resource Provider shall ensure that their User Information Security Management Systems are compatible with each other in respect of all the matters referred to in Sections G5.19 to G5.24.

## **G6. ANOMALY DETECTION THRESHOLDS: OBLIGATIONS ON THE DCC AND USERS**

### **Threshold Anomaly Detection Procedures**

G6.1 The "Threshold Anomaly Detection Procedures" shall be a SEC Subsidiary Document of that name which:

- (a) shall describe the means by which:
  - (i) each User shall be able securely to notify the DCC of the Anomaly Detection Thresholds set by that User, and of any exceptions that are applicable to each such Anomaly Detection Threshold;
  - (ii) the DCC shall be able securely to notify each User when a communication relating to that User is quarantined, or deleted from the DCC Systems, by the DCC; and
  - (iii) each such User shall be able securely to notify the DCC whether it considers that a communication which has been quarantined should be deleted from the DCC Systems or processed by the DCC;
- (b) shall determine the standard of security at which Users and the DCC must be able to notify each other in order for such notifications to be considered, for the purposes of paragraph (a), to have been given 'securely';
- (c) may make provision relating to the setting by Users and the DCC of Anomaly Detection Thresholds, including the issue of guidance by the DCC in relation to the appropriate level at which Anomaly Detection Thresholds should be set by Users; and
- (d) may make provision relating to the actions to be taken by Users and the DCC in cases in which an Anomaly Detection Threshold has been exceeded, which:

- (i) in the case of any SMETS1 Service Request which contains a data value that is inconsistent with a maximum or minimum set in accordance with paragraph (b)(ii) of the definition of Anomaly Detection Threshold in Section A1 (Definitions), shall include the deletion by the DCC of that Service Request and notification of the User that the deletion has taken place; and
- (ii) in any other case, may include provision for communications to be quarantined and remedial action to be taken.

### **Anomaly Detection Thresholds: Obligations on Users**

G6.2 Each User shall comply with any requirements of the Threshold Anomaly Detection Procedures which are applicable to it.

G6.3 Each User which is an Eligible User in relation to any one or more individual Services listed in the DCC User Interface Services Schedule:

- (a) shall, in respect of each User ID used by it in any User Role by virtue of which it is such an Eligible User, set Anomaly Detection Thresholds in respect of:
  - (i) the sum total of the number of Critical Commands and the number of SMETS1 Service Requests that are Critical Service Requests which relate to each such Service Reference Variant; and
  - (ii) the total number of Service Requests relating to each such Service Reference Variant in respect of which, if the relevant Device were a SMETS2+ Device, there are Service Responses that would contain Data of a type which is Encrypted in accordance with the GB Companion Specification; and
- (b) may, at its discretion, set other Anomaly Detection Thresholds.

G6.4 Where a User sets any Anomaly Detection Threshold in accordance with Section G6.3, it shall:

- (a) set that Anomaly Detection Threshold at a level designed to ensure that it will function, when used for the purposes of Threshold Anomaly Detection, as an effective means of detecting any Compromise to any relevant part of its User Systems;
- (b) before doing so, take into account any guidance issued by the DCC as to the appropriate level of the Anomaly Detection Threshold; and
- (c) after doing so, notify the DCC of that Anomaly Detection Threshold.

G6.4A Where, in accordance with the Common Test Scenarios Document, a User becomes an Eligible User for a User Role without successfully completing testing for a Critical Service Request which can potentially be sent by a User in that User Role, then the User must set an Anomaly Detection Threshold of zero in respect of that Critical Service Request.

### **Anomaly Detection Thresholds: Obligations on the DCC**

G6.5 The DCC shall comply with any requirements of the Threshold Anomaly Detection Procedures which are applicable to it.

G6.6 The DCC:



- (a) shall, for each individual Service Reference Variant listed in the DCC User Interface Services Schedule, set an Anomaly Detection Threshold in respect of:
    - (i) the sum total of the number of Critical Commands and the number of SMETS1 Service Requests that are Critical Service Requests which relate to that Service Reference Variant; and
    - (ii) the total number of Service Requests relating to that Service Reference Variant in respect of which, if the relevant Device were a SMETS2+ Device, there would be Service Responses containing Data of a type which is Encrypted in accordance with the GB Companion Specification;
  - (b) shall set an Anomaly Detection Threshold in respect of a data value that has been agreed with the Security Sub-Committee within each Signed Pre- Command relating to that Service Reference Variant and SMETS1 Service Request;
  - (c) shall set an Anomaly Detection Threshold in respect of the total number of each type of Critical Command that is not related to a Service Reference Variant listed in Appendix E (the DCC User Interface Services Schedule); and
  - (d) may, at its discretion, set other Anomaly Detection Thresholds.
- G6.6A The DCC shall, from no later than the ECoS Service Live Date, ensure that where an amended Anomaly Detection Threshold is notified in respect of any part of the DCC Live Systems, that amended Anomaly Detection Threshold shall only be applied in respect of that part of the DCC Live Systems following:
- (a) a successful Check Cryptographic Protection of the communication providing the notification of the amended Anomaly Detection Threshold in respect of that part of the DCC Live Systems; and
  - (b) confirmation that the communication providing the notification of the amended Anomaly Detection Threshold has not previously been the subject of a successful Check Cryptographic Protection in respect of that part of the DCC Live Systems.
- G6.7 Where the DCC sets any Anomaly Detection Threshold in accordance with Section G6.6, it shall:
- (a) set that Anomaly Detection Threshold at a level designed to ensure that it will function, when used for the purposes of Threshold Anomaly Detection, as an effective means of detecting any Compromise to any relevant part of the DCC Total System or of any User Systems; and
  - (b) before doing so consult, and take into account the opinion of, the Security Sub- Committee as to the appropriate level of the Anomaly Detection Threshold.
- G6.8 The DCC shall notify the Security Sub-Committee of:
- (a) each Anomaly Detection Threshold that it sets; and
  - (b) each Anomaly Detection Threshold that is set by a User and notified to the DCC in accordance with Section G6.4(c).
- G6.9 Where the DCC is consulted by a User in relation to an Anomaly Detection Threshold which that User proposes to set, the DCC shall:

- (a) provide to the User its opinion as to the appropriate level of that Anomaly Detection Threshold; and
- (b) in doing so, have regard to the need to ensure that it will function, when used for the purposes of Threshold Anomaly Detection, as an effective means of detecting any Compromise to any relevant part of the User Systems of that User.

### **Anomaly Detection Thresholds: Obligations on the DCC and Users**

G6.10 The DCC and each User shall, in relation to each Anomaly Detection Threshold that it sets:

- (a) keep the Anomaly Detection Threshold under review, having regard to the need to ensure that it continues to function, when used for the purposes of Threshold Anomaly Detection, as an effective means of detecting any Compromise to any relevant part of the DCC Total System and/or User Systems (as the case may be);
- (b) for this purpose have regard to any opinion provided to it by the Security Sub-Committee from time to time as to the appropriate level of the Anomaly Detection Threshold; and
- (c) where the level of that Anomaly Detection Threshold is no longer appropriate, set a new Anomaly Detection Threshold in accordance with the relevant provisions of this Section G6.

## **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);
  - (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).

G7.14 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:

- (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.

## Document Development and Maintenance

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;
- (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 that are proportionate and appropriate taking into consideration the security risks identified in the Security Risk Assessment; and
- (g) develop and maintain documents to be known as "**SSC Guidance for Device Security Assurance and Triage**" which shall set out the SSC's guidance on the requirements and processes to be followed in respect of Devices (including their 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 CPA Certification.

## 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;
- (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,
  - (c) and that person is referred to in this Section G8 as the “**User Independent Security Assurance Service Provider**”.
- G8.2 The Panel may appoint more than one person to carry out the functions of the User Independent Security Assurance Service Provider.

### **Scope of Security Assurance Services**

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

- (a) carry out User Security Assessments at such times and in such manner as is provided for in this Section G8;
- (b) produce User Security Assessment Reports in relation to Users that have been the subject of a User Security Assessment;
- (c) receive and consider User Security Assessment Responses and carry out any Follow-up Security Assessments at the request of the Security Sub-Committee;
- (d) otherwise, at the request of, and to an extent determined by, the Security Sub-Committee, carry out an assessment of the compliance of any User with its obligations under Sections G3 to G6 where:
  - (i) following either a User Security Self-Assessment or Verification User Security Assessment, any material increase in the security risk relating to that User has been identified; or
  - (ii) the Security Sub-Committee otherwise considers it appropriate for that assessment to be carried out;
- (e) review the outcome of User Security Self-Assessments;
- (f) at the request of the Security Sub-Committee, provide to it advice in relation to:
  - (i) the compliance of any User with its obligations under Sections G3 to G6 or any CPA Certificate Remedial Plan; 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) the requirements specified in Section G8.5; and
- (b) the requirements specified in Section G8.6.

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

- (a) is accredited by UKAS as meeting the requirements for providing audit and certification of information security management systems in accordance with ISO/IEC 27001:2013 (Information

Technology – Security Techniques – Information Security Management Systems) or any equivalent to that standard which updates or replaces it from time to time; and/or

- (b) holds another membership, accreditation, approval or form of professional validation that is in the opinion of the Security Sub-Committee substantially equivalent in status and effect to the arrangements described in paragraph (a).

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

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

#### Independence Requirement

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

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

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

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

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

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

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

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

#### Capacity Requirement

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

#### **Compliance of the User Independent Security Assurance Service Provider**

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

#### **Users: Duty to Cooperate in Assessment**

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

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

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

#### **Categories of Security Assurance Assessment**

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

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

- (c) a User Security Self-Assessment (as further described in Section G8.18); and
  - (d) a Follow-up Security Assessment (as further described in Section G8.19).
- G8.16 A **"Full User Security Assessment"** shall be an assessment carried out by the User Independent Security Assurance Service Provider in respect of a User to identify the extent to which that User is compliant with each of its obligations under Sections G3 to G6 in each of its User Roles.
- G8.17 A **"Verification User Security Assessment"** shall be an assessment carried out by the User Independent Security Assurance Service Provider in respect of a User to identify any material increase in the security risk relating to the Systems, Data, functionality and processes of that User falling within Section G5.14 (Information Security: Obligations on Users) since the last occasion on which a Full User Security Assessment was carried out in respect of that User.
- G8.18 A **"User Security Self-Assessment"** shall be an assessment carried out by a User, the outcome of which is reviewed by the User Independent Security Assurance Service Provider, to identify any material increase in the security risk relating to the Systems, Data, functionality and processes of that User falling within Section G5.14 (Information Security: Obligations on Users) since the last occasion on which a User Security Assessment was carried out in respect of that User.
- G8.19 A **"Follow-up Security Assessment"** shall be an assessment carried out by the User Independent Security Assurance Service Provider, following a User Security Assessment, in accordance with the provisions of Section G8.29.
- G8.20 For the purposes of Sections G8.17 and G8.18, a Verification Security Assessment and User Security Self-Assessment shall each be assessments carried out in respect of a User having regard in particular to:
- (a) any changes made to any System, Data, functionality or process falling within the scope of Section G5.14 (Information Security: Obligations on Users);
  - (b) where the User is a Supplier Party, any increase in the number of Enrolled Smart Metering Systems for which it is the Responsible Supplier; and
  - (c) where the User is a Network Party, any increase in the number of Enrolled Smart Metering Systems for which it is the Electricity Distributor or the Gas Transporter.

## **User Security Assessments: General Procedure**

### User Security Assessment Methodology

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

### The User Security Assessment Report

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

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

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

#### The User Security Assessment Response

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

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

G8.25 Where a User Security Assessment Report:

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

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

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



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

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

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

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

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

#### Follow-up Security Assessment

G8.29 Where a User Security Assessment Response sets out any steps that the User proposes to take in accordance with Section G8.26(b), and where those steps and the timetable within which it proposes to take them are accepted by the Security Sub-Committee, or alternative steps and/or an alternative timetable are agreed between it and the User in accordance with Section G8.27, the User Independent Security Assurance Service Provider shall, at the request of the Security Sub-Committee (and by such date as it may specify), carry out a Follow-up Security Assessment of the relevant User to:

- (a) identify the extent to which the User has taken the steps that have been accepted or agreed (as the case may be) within the timetable that has been accepted or agreed (as the case may be); and

- (b) assess any other matters related to the User Security Assessment Response that are specified by the Security Sub-Committee.

### **User Security Assessments: Further Provisions**

G8.30 The User Independent Security Assurance Service Provider:

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

### **Initial Full User Security Assessment: User Entry Process**

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

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

### **Initial Full User Security Assessment**

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

### **Panel: Setting the Assurance Status**

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

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

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

- (a) approved;
- (b) approved, subject to the Party:

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

#### Approval

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

- (a) a Party shall be considered to have successfully demonstrated that it meets the applicable security requirements of this Section G8 when:
  - (i) the Panel has set its assurance status to 'approved' in accordance with either Section G8.36(a) or (b); or
  - (ii) the Panel has set its assurance status to 'deferred' in accordance with Section G8.36(c) and the requirements specified in that Section have been met; and
- (b) the Panel shall notify the Code Administrator as soon as reasonably practicable after the completion of either event described in paragraph (a)(i) or (ii).

#### Obligations on an Approved Party

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

#### Disagreement with Panel Decisions

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

## Security Assurance Assessments: Post-User Entry Process

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

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

### Supplier Parties

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

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

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

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

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

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

G8.43 In assessing for the purposes of Sections G8.41 and G8.42 the number of Domestic Premises and Non-Domestic Premises supplied with electricity and/or gas through one or more Smart Metering Systems

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

#### Network Parties

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

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

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

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

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

#### Other Users

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

- (a) within 12 months after the previous User Security Verification Assessment, schedule a User Security Self-Assessment;

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

### Interpretation

G8.48 Section G8.49 applies where:

- (a) pursuant to Sections G8.41 to G8.43, it is necessary to determine, in relation to any Supplier Party, the number of Domestic Premises and Non-Domestic Premises that are supplied with electricity and/or gas through one or more Smart Metering Systems for which it is the Responsible Supplier; or
- (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 SEC Section G or any CPA Certificate Remedial Plan; and
  - (ii) changes in security risks relating to the Systems, Data, functionality and processes of the DCC which fall within SEC Section G5 (Information Security: Obligations on the DCC);
- (f) at the request of the Security Sub-Committee, provide to it advice in relation to the suitability of any remedial action plan for the purposes of Section M8.4 of the Code (Consequences of an Event of Default);
- (g) at the request of the Security Sub-Committee Chair, provide a representative to attend and contribute to the discussion at any meeting of the Security Sub-Committee; and
  - (i) undertake such other activities and do so at such times and in such manner, as may be further provided for in this Section G9;
  - (ii) assess the DCC's compliance with the requirements of Condition 8 (Security Controls for the Authorised Business) of the DCC Licence;
  - (iii) such other requirements relating to the security of the DCC Total System as may be specified by the Security Sub-Committee or the Panel from time to time.

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

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

#### **The DCC Independent Security Assessment Service Provider**

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

- (a) of the scope specified in Section G9.2;
- (b) from a person who:
  - (i) is suitably qualified in accordance with Section G9.5;
  - (ii) is suitably independent in accordance with Section G9.8.

#### **Suitably Qualified Service Provider**

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

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

- G9.6 The requirements specified in this Section G9.6 are that the DCC Independent Security Assessment Service Provider:
- (a) is accredited by UKAS as meeting the requirements for providing audit and certification of information security management systems in accordance with ISO/IEC 27001:2017 Information Technology – Security Techniques – Information Security Management Systems) or any equivalent to that standard which updates or replaces it from time to time; and/or
  - (b) holds another membership, accreditation, approval or form of professional validation that is in the opinion of the Security Sub-Committee substantially equivalent in status and effect to the arrangements described in paragraph (a).
- G9.7 The requirement specified in this Section G9.7 is that the DCC Independent Security Assessment Service Provider:
- (a) employs consultants who are assured under an official cyber security qualification scheme recognised by NCSC or the UK Cyber Security Council or UKAS and which is approved by the Security Sub-Committee at levels equivalent to 'Chartered', 'Principal', 'Lead' or 'Senior Practitioner' in either 'Security and Information Risk Advisor' or 'Information Assurance Auditor' roles; and
  - (b) engages those individuals as its lead auditors for the purposes of carrying out all security assessments in accordance with this Section G7.

### **Independence Requirement**

- G9.8 The DCC Independent Security Assurance Service Provider shall be treated as suitably independent in accordance with this Section G9.8 only if it satisfies:
- (a) the requirements specified in Section G9.9; and
  - (b) the requirement specified in Section G9.10.
- G9.9 For the purposes of Sections G9.9 and G9.10:
- (a) the DCC must be independent from the DCC Independent Security Assessment Service Provider in carrying out functions under this Section G9; and
  - (b) all of the DCC's Service Providers must be independent from the DCC Independent Security Assessment Service Provider in carrying out its functions to assess the DCC's compliance with its obligations as the DCC under Sections G2 and G4 to G6 and DCC Licence Condition 8 (Security Controls for the Authorised Business) and SEC Appendix Z Sections 6 and 7.
- G9.10 The requirements specified in this Section G9.10 are that:
- (a) neither the DCC or any of its subsidiaries, and no DCC Service Provider or any of its subsidiaries, holds or acquires any investment by way of shares, securities or other financial rights or interests in the DCC Independent Security Assessment Service Provider;
  - (b) no director of the DCC and no director of any DCC Service Provider, is or becomes a director or employee of, or holds or acquires any investment by way of shares, securities or other financial rights or interests in, the DCC Independent Security Assessment Service Provider; and

- (c) the DCC Independent Security Assessment Service Provider does not hold or acquire a participating interest (as defined in section 421A of the Financial Services and Markets Act 2000) in the DCC or any of the DCC's Service Providers, (for these purposes references to the DCC's Service Providers shall not include the DCC Independent Security Assessment Service Provider where it acts in that capacity).

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

### **Compliance of the DCC Independent Security Assessment Service Provider**

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

### **DCC: Duty to Cooperate in Assessment**

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

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

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

### **Categories of DCC Security Assessment**

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

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

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

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

## **DCC Security Assessments: General Procedure**

### **DCC Security Assessment Methodology**

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

### **The DCC Security Assessment Report**

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

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

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

### **The DCC Security Assessment Response**

- G9.21 Following the receipt by the DCC of a DCC Security Assessment Report which relates to it, the DCC shall as soon as reasonably practicable, and in any event by no later than such date as the Security Sub-Committee may specify:
- (a) produce a written response to that report (a "**DCC Security Assessment Response**") which addresses the findings set out in the report; and
  - (b) submit a copy of that response to the Security Sub-Committee and the DCC Independent Security Assessment Service Provider.
- G9.22 Where a DCC Security Assessment Report following a Full DCC Security Assessment, specifies any instance of actual or potential non-compliance of the DCC with its obligations under Sections G2 and G4 to G6 and/or with DCC Licence Condition 8 (Security Controls for the Authorised Business) and/or with SEC Appendix Z, Sections 6 and 7, the DCC shall ensure that its DCC Security Assessment response includes the matters referred to in Section G9.23.
- G9.23 The matters referred to in this Section are that the DCC Security Assessment Response:
- (a) indicates whether the DCC accepts the relevant findings of the DCC Independent Security Assessment Service Provider and, where it does not, explains why this is the case;
  - (b) sets out any steps that the DCC has taken or proposes to take in order to remedy and/or mitigate the actual or potential non-compliance or the increase in security risk (as the case may be) specified in the DCC Security Assessment Report; and
  - (c) identifies a timetable within which the DCC proposes to take any such steps that have not already been taken.
- G9.24 Where a DCC Security Assessment Response sets out any steps that the DCC proposes to take in accordance with Section G9.23(b), the Security Sub-Committee (having considered the advice of the DCC Independent Security Assessment Service Provider) shall review that response and either:
- (a) notify the DCC that it accepts that the steps that the DCC proposes to take, and the timetable within which it proposes to take them, are appropriate to remedy and/or mitigate the actual or potential non-compliance or increase in security risk (as the case may be) specified in the DCC Security Assessment Report; or
  - (b) seek to agree with the DCC such alternative steps and/or timetable as would, in the opinion of the Security Sub-Committee, be more appropriate for that purpose.
- G9.25 Where a DCC Security Assessment Response sets out any steps that the DCC proposes to take in accordance with Section G9.23(b), and where those steps and the timetable within which it proposes to take them are accepted by the Security Sub-Committee, or alternative steps and/or an alternative timetable are agreed between it and the DCC in accordance with Section G9.24(b), the DCC shall:
- (a) take the steps that have been accepted or agreed (as the case may be) within the timetable that has been accepted or agreed (as the case may be); and
  - (b) report to the Security Sub-Committee on:
    - (i) its progress in taking those steps, at any such intervals or by any such dates as the Security Sub-Committee may specify;

- (ii) the completion of those steps in accordance with the timetable; and
- (iii) any failure to complete any of those steps in accordance with the timetable, specifying the reasons for that failure.

#### Follow-up Security Assessment

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

#### DCC Security Assessments: Further Provisions

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

#### Setting the Compliance Status

- G9.28 Following the completion of a Full DCC Security Assessment, the Security Sub-Committee shall consider the DCC Security Assessment Report and the DCC Security Assessment Response.
- G9.29 The Security Sub-Committee shall identify whether any remaining non-compliances that exist with Section G2 or G4 to G6 and/or the DCC Licence Condition 8 (Security Controls for the Authorised Business) and/or SEC Appendix Z, Sections 6 and 7 and shall, where appropriate:
- (a) note and record that there are no non-compliances; or
  - (b) note and record the specific non-compliances that need to be addressed.
- G9.30 Where the Security Sub-Committee identifies remaining non-compliances that exist with Section G2 and G4 to G6 and/or the DCC Licence Condition 8 (Security Controls for the Authorised Business) and/or SEC Appendix Z Sections 6 and 7, it shall:
- (a) require the DCC to take the steps set out in Section G9.24: or
  - (b) require a Follow-up Security Assessment as set out in Section G9.26.
- G9.31 Where the Security Sub-Committee identifies any remaining non-compliances with Section G2 or G4 to G6 and/or the DCC Licence Condition 8 (Security Controls for the Authorised Business) and/or SEC Appendix Z, Sections 6 and 7, it shall notify the Panel as required by G9.37(b).

## CPA Certificate Remedial Plan Preparation

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

### Disagreement with Security Sub-Committee Decisions

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

## Events of Default

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

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

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

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

G9.38 Where the Security Sub-Committee has:

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

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

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

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

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



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

#### **CPA Certificate Remedial Plan Preparation**

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

### **G10. SHARED RESOURCES**

G10.1 Where any resources which form part of the User Systems of a User also form part of the User Systems of any one or more other Users, those resources shall be known as "**Shared Resources**".

G10.2 For the purposes of this Part G, a "**Shared Resource Provider**" shall mean any Party which makes available Shared Resources to one or more Users, for use by them or on their behalf, in accordance with any agreement entered into or arrangement made with each such User.

#### **Shared Resources which constitute the entirety of User Systems**

G10.3 A User may not employ Shared Resources which:

- (a) are made available to it by one other person; and
- (b) constitute the entirety of its User Systems,

unless those Shared Resources are provided by a Shared Resource Provider.

#### **Obligations on Shared Resource Providers**

G10.4 Each Shared Resource Provider shall:

- (a) maintain a list of every User to which it makes available Shared Resources in accordance with an agreement or arrangement of the type described in Section G10.2;
- (b) revise that list from time to time to ensure that it remains accurate and up to date at all times;
- (c) submit to the Security Sub-Committee a copy of that list and of any revision to it, so that the Security Sub-Committee is in possession of a copy of that list that is accurate and up to date at all times.

G10.5 For the purposes of Sections G1 to G5 and G7 to G9, unless the context otherwise requires, a Shared Resource Provider shall be treated as if it were a User, and:

- (a) any reference to a User shall be deemed to include a reference to that Shared Resource Provider;
- (b) subject to Section G10.6, obligations in those Sections which are expressed to apply to a User shall apply to that Shared Resource Provider;
- (c) references in those obligations to User Systems shall be deemed, for the purpose of their application to the Shared Resource Provider, to be references to the Shared Resources which it provides; and

- (d) the role of the Shared Resource Provider shall be treated as if it were an additional category of User Role.

### **Continuing Obligations of Users**

G10.6 Section G10.5 shall have effect without prejudice to the duty of Users to comply with the obligations at Sections G1 to G5 and G7 to G9, so that, where a Shared Resource Provider provides a User with Shared Resources constituting its User Systems, both it and the User shall be jointly and severally liable for any failure to comply with an obligation which relates to those Shared Resources, subject to:

- (a) Section G5.28 which has effect for determining the obligations of, and the relationship between, the User and the Shared Resource Provider in relation to their respective User Information Security Management Systems; and
- (b) Sections G8.61 to G8.63 which have effect for determining:
  - (i) when the Shared Resource Provider is required to schedule either a User Security Assessment or User Security Self-Assessment; and
  - (ii) how the outcome of a User Security Assessment in respect of the Shared Resource Provider is applicable to a User to which that Shared Resource Provider is providing Shared Resources.

### **Additional Obligations following User Security Assessments**

G10.7 Section G10.8 applies, following a User Security Assessment that has been carried out in respect of a Shared Resource Provider, in relation to the information to be provided to each User with which, at that time, the Shared Resource Provider has an agreement or arrangement of the type described in Section G10.2 (a "Shared Resource User").

G10.8 Where this paragraph applies:

- (a) the User Independent Security Assurance Service Provider shall (in addition to its obligation at Section G8.23) submit a copy of the User Security Assessment Report to each Shared Resource User;
- (b) the Shared Resource Provider shall (in addition to its obligation at Section G8.24) submit a copy of its User Security Assessment Response to each Shared Resource User;
- (c) the Security Sub-Committee shall (in addition to its obligation at Section G8.27) notify each Shared Resource User of any steps accepted or agreed (as the case may be) with the Shared Resource Provider; and
- (d) the Shared Resource Provider shall (in addition to its obligation at Section G8.28(b)) provide each Shared Resource User with a copy of any report that is submitted from time to time to the Security Sub-Committee in accordance with Section G8.28(b).

### **Interpretation**

G10.9 For the purposes of Sections G1 to G5 and G7 to G9, unless the context otherwise requires, any expressions which are:

- (a) defined in those Sections by reference to a User or User Systems; or
- (b) defined in Section A by reference to a User or User Systems, and used in those Sections,

shall be interpreted so that any reference to a User is deemed to include a reference to a Shared Resource Provider, and any reference to User Systems is deemed, in the case of a Shared Resource Provider, to be a reference to the Shared Resources provided by it.

## **G11. THE ECOS TRANSITION AND MIGRATION APPROACH DOCUMENT**

### **Overview**

- G11.1 The first version of the ECoS Transition and Migration 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).
- G11.2 The second (and each subsequent version as may be required) of the ECoS Transition and Migration Approach Document is to be developed by the DCC pursuant to this Section G11, and incorporated into this Code pursuant to Part G of Condition 22 of the DCC Licence and, where Section X continues to be in effect, Section X5 (Incorporation of Certain Documents into this Code).

### **Purpose of the ECoS Transition and Migration Approach Document**

- G11.3 The purpose of the first version of the ECoS Transition and Migration Approach Document is to provide that the modifications made to this Section G and to Section L of the Code for the purposes of setting out the arrangements which are to apply following the completion of ECoS Migration, shall not apply in respect of any period which is prior to:
  - (a) the commencement of ECoS Migration; and
  - (b) the point in time at which Devices with Device Security Credentials that comprise (in part) information from an ECoS Certificate may be Commissioned.
- G11.4 In addition to the purpose set out in Section G11.3, the purposes of the second (and each subsequent) version of the ECoS Transition and Migration Approach Document are to:
  - (a) enable the ECoS Migration of SMETS2+ Devices such that the Device Security Credentials for such Devices comprise (in part) information from an ECoS Certificate instead of information from a TCoS Certificate;
  - (b) facilitate the processing of a 'CoS Update Security Credentials' Service Request made by the TCoS Service Provider in respect of any Device that has not ECoS Migrated;
  - (c) permit, for a transitional period, the installation of Devices in respect of which the Device Security Credentials are comprised (in part) by information from a TCoS Certificate;
  - (d) provide for additional and/or varied provisions to apply for a transitional period prior to, during and/or following the ECoS Migration of Devices; and
  - (e) provide for additional and/or varied provisions to apply for a transitional period to manage the interactions between the Enduring Change of Supplier Arrangements and the introduction of the

Centralised Registration Service, which may take place prior to, during, or following the commencement of ECoS Migration.

### **Content of the ECoS Transition and Migration Approach Document**

G11.5 The ECoS Transition and Migration Approach Document may include, without limitation, some or all of the following:

- (a) rights and/or obligations of the DCC and other Parties designed to facilitate or achieve the purposes of the ECoS Transition and Migration Approach Document which are either additional to or vary other rights and/or obligations set out in this Code;
- (b) the processes by which SMETS2+ Devices that have been Commissioned will have their Device Security Credentials updated such that those security credentials which relate to the CoS Party will be derived from information contained in an ECoS Certificate instead of information contained in a TCoS Certificate;
- (c) the processes by which changes to DCC Systems are to be made to enable the DCC to begin processing “CoS Update Security Credentials” Service Requests in relation to SMETS1 Devices;
- (d) pre-conditions to apply in relation to the ECoS Migration of any SMETS1 or SMETS2+ Device, including by reference to the DCC, the Device Model, and/or the Responsible Supplier;
- (e) provisions enabling the DCC to process a 'CoS Update Security Credentials' Service Request in a different way, method or manner depending upon whether or not the Device in respect of which the Service Request is made has been ECoS Migrated;
- (f) provisions that, from any such date as may be specified, permit or require any newly installed or Commissioned Device to have security credentials which relate to the CoS Party to be derived from the information contained in an ECoS Certificate instead of information that is contained in a TCoS Certificate;
- (g) provisions requiring the DCC to report on its progress on ECoS Migration, including identifying whether in relation to Devices any particular category of Device Model and/or Device Type has failed, or is more likely to fail, ECoS Migration;
- (h) provisions requiring the DCC to apply a specific strategy in respect of attempting to complete ECoS Migration for a Device in respect of which ECoS Migration has previously failed;
- (i) provisions requiring the DCC and Supplier Parties to take steps to resolve matters that are causing, or contributing to the cause of, failures of ECoS Migration;
- (j) provisions requiring the secure decommissioning of Systems of the TCoS Service Provider, for the revocation of any associated Organisation Certificates, and for the verifiable destruction of associated Private Keys;
- (k) limitations and/or variations to the Services and/or the rights and/or obligations of the Parties to apply for a transitional period prior to and/or following the ECoS Migration of some or all Devices, which may include limitations and/or variations to Services in light of other proposed changes to this Code; and

- (l) provision for the referral and determination of disputes in respect of the ECoS Transition and Migration Approach Document, which may include interim or final determinations by the Secretary of State, the Authority, the Panel or any other person specified by the Secretary of State.

### Process to Develop Second (and any subsequent) Document for Designation

G11.6 The DCC shall, where so directed by the Secretary of State from time to time, develop and consult upon the second (and any subsequent) version of the ECoS Transition and Migration Approach Document and submit it to the Secretary of State in accordance with the following process:

- (a) the DCC shall, in consultation with the Parties, such other persons as are likely to be interested, and where Section G11.7 applies, the Security Sub-Committee, produce a draft of the document;
- (b) where a disagreement arises with any Party or other person with regard to any proposal as to the content of the document, the DCC shall endeavour to reach an agreed proposal with that person consistent with the purposes of the ECoS Transition and Migration Approach Document;
- (c) the DCC shall send a copy of the draft document to the Secretary of State as soon as is practicable after completion of the process described in paragraphs (a) and (b) above, and shall when doing so provide to the Secretary of State:
  - (i) a statement of the reasons why the DCC considers that draft to be fit for purpose;
  - (ii) copies of the consultation responses received; and
  - (iii) a summary of any disagreements that arose during consultation and that have not been resolved by reaching an agreed proposal;

G11.7 Where the DCC reasonably believes that any changes to a version of the ECoS Transition and Migration Approach Document it is developing in accordance with Section G11.6 might be considered to have an impact upon on the End-to-End Security Architecture or the risks identified in the Security Risk Assessment:

- (a) the DCC shall submit to the Security Sub-Committee for its review and comment an impact assessment that sets out the DCC's views of any such impact (a **Security Impact Assessment**);
- (b) the Security Sub-Committee shall provide any comments or observations that they have on the Security Impact Assessment to the DCC;
- (c) the DCC shall provide a response to any such comments or observations to the Security Sub-Committee and update the relevant draft of the ECoS Transition and Migration Approach Document as appropriate to take into account the comments or observations; and
- (d) following the DCC's response, the Security Sub-Committee shall notify the Secretary of State whether it considers there to be any remaining outstanding unacceptable risks to the End-to-End Security Architecture as a consequence of the proposed changes to the ECoS Transition and Migration Approach Document.

G11.8 The DCC shall comply with any direction given to it by the Secretary of State following the Secretary of State's consideration of the draft document which direction may require the DCC to:

- (a) make such amendments to the draft document as are set out or described in the direction;

- (b) produce and submit to the Secretary of State a further draft of the document; and
- (c) follow a specified process (and the time within which that process shall be completed) prior to submitting a further draft of the document to the Secretary of State.

### **Application of the ECoS Transition and Migration Approach Document**

G11.9 The DCC and the categories of Party referred to in the ECoS Transition and Migration Approach Document shall comply with the ECoS Transition and Migration Approach Document.

G11.10 The ECoS Transition and Migration Approach Document shall have priority over the other SEC Subsidiary Documents in relation to the subject matter of the ECoS Transition and Migration Approach Document.

### **Expiry of each version of the ECoS Transition and Migration Approach Document**

G11.11 The second, and each subsequent, version of the ECoS Transition and Migration Approach Document shall provide for a date (or a mechanism for determining a date) from which that version is to no longer apply. From such date, that version of the ECoS Transition and Migration Approach Document shall no longer have any effect (but without prejudice to the rights and obligations arising prior to that date) and it shall automatically be deleted from this Code.

### **Definitions**

G11.12 For the purposes of this Section G11:

<b>Centralised Registration Service</b>	has the meaning given to that term in Condition 1 of the DCC Licence.
<b>ECoS Certificate</b>	means an Organisation Certificate for which the ECoS Service Provider is the Subject.
<b>ECoS Migration</b>	means, in relation to any one or more Device(s), that the Device Security Credentials held on or in relation to any such Device previously populated with information from a TCoS Certificate have been populated with information from an ECoS Certificate, and the expression “ <b>ECoS Migrated</b> ” shall be interpreted accordingly.
<b>ECoS Service Provider</b>	means each DCC Service Provider that, following the completion of the implementation of the Enduring Change of Supplier Arrangements, supports or is to support the performance of tasks ascribed to the CoS Party.
<b>Enduring Change of Supplier Arrangements</b>	has the meaning given to that term in Condition 13A of the DCC Licence.
<b>Subject</b>	has the meaning given to that term in Annex A of Appendix B (Organisation Certificate Policy).
<b>TCoS Certificate</b>	means an Organisation Certificate for which the TCoS Service Provider is the Subject.

<b>TCoS Service Provider</b>	means the DCC Service Provider that, prior to the commencement of the implementation of the Enduring Change of Supplier Arrangements, is the service provider that supports the performance of tasks ascribed to the CoS Party.
------------------------------	---

## **G12. SECURITY ASSURANCE OF DEVICE TRIAGE FACILITIES**

G12.1 Some of the expressions used in this Section G12 are defined in Section G12.9.

G12.2 Where the SSC Guidance for Device Security Assurance and Triage specifies that independent assurance of Triage Facility Providers is required to achieve appropriate levels of security assurance in accordance with the requirements of this Code, this Section G12 shall apply.

### **Triage Facility Provider Obligations**

G12.3 In order to become a Triage Facility Provider, an entity must either be an existing Party or accede to this Code and become a Party. A Triage Service Provider is not required to be a User.

G12.4 Each Triage Facility Provider shall:

- (a) not attempt to undertake Triage Activities on any Device where the tamper-protection boundary required by the CPA Security Characteristics has already been breached before reaching the Triage Facility (taking into account any allowable breaches necessary as part of essential Device maintenance and/or the de-commissioning process);
- (b) only use the Triage Tool and Triage System Interface provided by a Device's Manufacturer to access the Manufacturer's Triage System and not use any other electronic devices, interfaces or IT systems for carrying out Triage Activities;
- (c) ensure multi-factor authentication and role-based access controls are used within its Triage Facility to control access to the graphical user interface (GUI) of the Triage Tool, and to control access to the Triage System Interface;
- (d) at all times prevent unauthorised use of the Triage Tool and Triage System Interface, and ensure the physical security of the Triage Tool and any Devices that are subject to Triage Activities;
- (e) ensure that all the required tamper-protection seals are fitted to Devices on completing the Triage Activities;
- (f) maintain an asset management system to record Triage Activities undertaken at the Triage Provider's Triage Facility, including details of:
  - (i) the Requestor of any change to the configuration of a Device;
  - (ii) the Device Model and serial number of each Device where the tamper-protection boundary is breached in order to undertake (or attempt to undertake) Triage Activities;
  - (iii) details of Triage Activities successfully undertaken;

- (iv) details of any failed attempts to complete Triage Activities; and
  - (v) confirmation that any seals and tamper-protection required by the CPA Security Characteristics have been applied before returning a Device to a Requestor.
- (g) when requested by the Security Sub-Committee, provide the Security Sub-Committee with an up-to-date copy of the records maintained pursuant to Section G12.3(f);
  - (h) provide all reasonable assistance that may be requested by the Security Sub-Committee or the User Independent Security Assurance Service Provider for the purposes of conducting a User Security Assessment;
  - (i) subject to Section G12.5, comply with the requirements of Sections G1, G3 to G5, G7 and G8;
  - (j) comply with the requirements of Sections G12.6 to G12.8; and
  - (k) act in accordance with Good Industry Practice.
- G12.5 For the purposes of Sections G1, G3 to G5, G7 and G8, unless the SSC Guidance for Device Security Assurance and Triage states otherwise, a Triage Facility Provider shall be treated as if it is a User and:
- (a) any reference to a 'User' shall be deemed to include a reference to a 'Triage Facility Provider';
  - (b) except for where the SSC Guidance for Device Security Assurance and Triage states otherwise, obligations in those Sections which are expressed to apply to a User shall apply to a Triage Facility Provider;
  - (c) references in those obligations to 'User Systems' shall be deemed, for the purpose of their application to the Triage Facility Provider, to be references to the Triage Activities undertaken at the Triage Facility; and
  - (d) the Security Sub-Committee shall provide Triage Facility Providers and other Parties with guidance on interpretation of Sections G1, G3 to G5, G7 and G8 in respect of their application to Triage Facility Providers and Triage Activities.

### **User Security Assessments of Triage Facilities**

- G12.6 Prior to undertaking any Triage Activities, each Triage Facility Provider shall be subject to an initial Full User Security Assessment by a User Independent Security Assurance Service Provider following the process in Sections G8.22 to G8.30.

### **Approval**

- G12.7 On receipt of the initial Full User Security Assessment Report and the User Security Assessment Response, the assurance status shall be set in accordance with Sections G8.35 to G8.36 and:
- (a) where the assurance status is set to 'approved' under Section G8.36(a) then the Triage Facility Provider may undertake Triage Activities as set out in the SSC Guidance for Device Security Assurance and Triage;



- (b) where the assurance status is set to 'approved' subject to conditions (as set under Section G8.36(b)) then the Triage Facility Provider will require explicit approval from the Security Sub-Committee before undertaking Triage Activities; and
- (c) where the assurance status is 'deferred' or 'rejected' under Section G8.36(c) or (d), respectively, then the Triage Facility Provider is not approved to undertake Triage Activities.

## Second and subsequent User Security Assessments

G12.8 Within 12 months following completion of the initial and each subsequent User Security Assessment, the Triage Facility Provider shall schedule a subsequent User Security Assessment with the User Independent Security Assurance Provider. The Security Sub-Committee shall determine the category of each such User Security Assessment to be carried out and, in doing so shall:

- (a) consider any security risks identified during or since the previous User Security Assessment;
- (b) take account of the volume of Devices for which Triage Activities are carried out; and
- (c) reach a determination based on a proportionate assessment of the security risks as to whether the next User Security Assessment should be:
  - (i) a Full User Security Assessment;
  - (ii) a Verification User Security Assessment; or
  - (iii) a User Security Self-Assessment.

## Definitions

G12.9 For the purpose of this Section G12:

<b>Requestor</b>	means an entity (such as a Party or a meter asset provider) that requests that Triage Activities are undertaken by a Triage Facility Provider.
<b>SSC Guidance for Device Security Assurance and Triage</b>	means the document published by the Security Sub-Committee under Section G7.19(g), which sets out guidance on the requirements and processes (including security controls and security assurance) to be followed by Triage Facility Providers undertaking Triage Activities.
<b>Triage</b>	means the diagnosis, upgrading or resetting of a Device.
<b>Triage Activities</b>	means any Triage-related activity carried out in circumstances where the SSC Guidance for Device Security Assurance and Triage requires independent assurance, including in such circumstances: <ul style="list-style-type: none"> <li>a) the breach of the tamper-protection boundary;</li> <li>b) any unlocking of internal non-operational ports;</li> <li>c) any changes to the configuration of the Device Data;</li> <li>d) confirmation of the firmware version on the Device when Triage has been completed; and</li> <li>e) completion of Triage by replacing all internal non-operational port</li> </ul>

	seals required pursuant to the CPA Security Characteristics and all tamper-protection boundary seals.
<b>Triage Facility</b>	means a premises where Triage Activities are undertaken.
<b>Triage Facility Provider</b>	means a Party which operates a Triage Facility for the purpose of carrying out Triage Activities.
<b>Triage System Interface</b>	<p>means a secure virtual private network, encrypted link provided by a Manufacturer in order to connect its Triage System to a Triage Tool at a Triage Facility, which provides confidentiality and integrity of communications. The Triage System Interface:</p> <ul style="list-style-type: none"> <li>• Must use either TLS or IPsec, and</li> <li>• If using TLS then must include client authentication.</li> </ul>
<b>Triage System</b>	means a secure IT system established for the purposes of Triage and operated by a Manufacturer, as part of its Device manufacturing capability, which the Triage Facility Provider connects to using the Triage Tool and Triage System Interface, and which is compliant with the requirements of the NCSC Commercial Product Assurance (CPA) Scheme and the associated CPA Security Characteristics.
<b>Triage Tool</b>	means an electronic device provided by a Manufacturer, which is used to Triage Devices in accordance with SSC Guidance for Device Security Assurance and Triage, and which is cryptographically authorised such that it can only be used for Triage Activities and cannot be given additional capabilities by an operator in a Triage Facility.