SECTION G - SECURITY

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, promptly notify the Panel and the Security Sub-Committee.

System Design and Operation

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 service provider 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 Sections G2.21 and G2.22, each DCC Individual Live System is Separated from each other such System.

G2.21 The DCC Individual Live System referred to at paragraph (c) of the definition of DCC Live Systems in Section A1 (Definitions) need not be Separated from the DCC Individual Live System referred to at paragraph (a) of that definition to the extent that it uses that System referred to at paragraph (a) solely for the purposes of confirming the relationship between:

(a) an MPAN or MPRN and any Party Details;

(b) an MPAN or MPRN and any Device; or

(c) any Party Details and any User ID.

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 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, CESG Good Practice Guide 18:2012 (Forensic Readiness), or any equivalent to that CESG Good Practice Guide which updates or replaces it from time to time.

G2.28 The DCC shall monitor the DCC Systems in compliance with:

(a) CESG Good Practice Guide 13:2012 (Protective Monitoring); or

(b) any equivalent to that CESG Good Practice Guide which updates or replaces it from time to time.

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;

Deleted: or

(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

Deleted: ,

(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 SMETS 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.

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:

(i) take into account any guidance issued by the DCC as to the appropriate level of the Anomaly Detection Threshold; and

(ii) have regard in particular to the forecast number of Service Requests provided by the User to the DCC in accordance with Section H3.22 (Managing Demand for User Interface Services); and

(c) after doing so, notify the DCC of that Anomaly Detection Threshold.

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;

Deleted: and

(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.

G6.7 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.