SEC
Smart Energy Code

This document is classified as **White** in accordance with the Panel Information Policy. Information can be shared with the public, and any members may publish the information, subject to copyright.

MP115

‘Changes to the NCSC Good Practice Guides’

Modification Report

Version 1.0

Corporate member of Plain English Campaign
Committed to clearer communication
592

About this document

This document is a Modification Report. It currently sets out the background, issue, solution, impacts, costs, implementation approach and progression timetable for this modification, along with any relevant discussions, views and conclusions.

Contents

This document also has one annex:

- **Annex A** contains the redlined changes to the Smart Energy Code (SEC) required to deliver the Proposed Solution.

Contact

If you have any questions on this modification, please contact:

Joe Hehir

020 7770 6874

Joe.hehir@gemserv.com

1. Summary

This proposal has been raised by Gordon Hextall on behalf of the Smart Metering Key Infrastructure (SMKI) Policy Management Authority (PMA).

A Smart Energy Code Administrator and Secretariat (SECAS) review of the SMKI Document Set has found that it contains several references to Good Practice Guides (GPGs) that have been discontinued and will not be replaced. The SMKI PMA wishes to address this by aligning the SEC with these changes and by making available authorised replacement SMKI PMA guidance. If this issue is not addressed, the SEC will contain several references to GPGs that are no longer live or are subject to frequent change outside of SMKI PMA control.

In addition, the Proposer wishes to include provisions for updated or replacement standards, procedures and guidelines in relation to the SMKI Document Set in the SEC. This is also the case for the transitional periods for such documents. This would remove ambiguity and facilitate the efficient implementation of this Code by giving Parties a transitional period to comply with any updated or replacement guidance in relation to the SMKI Document Set.

This modification is expected to cost £2,400 and impact all SEC Party categories.

The targeted implementation date is 5 November 2020 (November 2020 SEC Release).

2. Issue

What are the current arrangements?

Standards, procedures and guidelines

The SEC contains numerous references to standards procedures and guidelines, specifically in relation to security architecture of the End-to-End Smart Metering System[1]. These include GPGs, International Organization for Standardization (ISO) standards, Federal Information Processing Standards (FIPS) and Request for Comments (RFCs). These assist the DCC and SEC Parties to achieve consistent standards in the application of security controls and in the understanding of complying with such standards.

What are the GPGs?

GPGs were developed by the National Cyber Security Centre (NCSC) (formerly the Communications-Electronics Security Group (CESG)). These guides assisted UK industries to achieve consistent standards in the application of security controls and the protection of Critical National Infrastructure (CNI).

The SEC contains references to several NCSC GPGs that are mandated, mainly for compliance by the DCC. The DCC has ensured that the obligation for compliance with the GPGs have been enshrined into the contracts with its Service Providers.

What is the issue?

SECAS review of the SMKI Document Set

GPGs

At the request of the SMKI PMA, SECAS has recently conducted a review of the standards and guidance in the SMKI Document Set and has identified the following:

- GPG 13 ‘Protective Monitoring for HMG ICT Systems’ has been discontinued by the NCSC (although the document is still available on the NCSC website).
- GPG 43 ‘Secure Design of On-Line Public Services’ has been discontinued and has been removed from the NCSC website (although it is still available on the gov.uk website).
- GPG 45 ‘Identity proofing and verification of an individual’ was updated (by the Government Digital Service (GDS) on 15 April 2019 and again on 17 December 2019.
- GPG 46 ‘Identity assurance: Organisation identity’ is no longer on the NCSC website. It is still on the gov.uk website but must be discontinued since it refers to GPG 43 and an old version of GPG 45.

Further to this, the Proposer has also found that GPG 18 ‘Forensic Readiness’ has also been discontinued by the NCSC.

---

[1] The DCC Total System, all Enrolled Smart Metering Systems, all User Systems and all RDP Systems.

The NCSC response

The NCSC has confirmed that it has discontinued GPGs and has moved to greater use of blogs. It recommends:

- https://www.ncsc.gov.uk/blog-post/keeping-your-security-monitoring-effective
- https://www.ncsc.gov.uk/blog-post/learning-love-logging
- https://www.ncsc.gov.uk/blog-post/security-and-usability--you-can-have-it-all-
- https://www.ncsc.gov.uk/collection/cyber-security-design-principles

All the NCSC guidance can be found by topic at:

- https://www.ncsc.gov.uk/section/advice-guidance/all-topics

The NCSC justified the continued presence of GPG 13 on the NCSC website saying:

> *"it is there for historical reference but in line with changes to the Government's approach to risk management, GPG 13 is mainly replaced with other guidance because of concerns that departments were incorrectly interpreting what was intended to be guidance, as mandatory government policy.* ***This frequently led to the control framework laid out in GPG 13 being mandated in contracts or being followed literally by systems implementers*** *without any consideration of the business context in which a particular system was operating."*

The bold text shows how it was incorporated (originally with CESG support) into the SEC and the related contracts with the DCC's Service Providers.

Recently updated GPG 45 is on the gov.uk website but is now under the ownership of the GDS, which is responsible for the Government Gateway and the 'GOV.UK Verify' service.

The NCSC has stated that blogs can be kept up to date more easily. Unfortunately, these are inappropriate to use as SEC references as they are not written in the context of smart metering.

Updated or replacement standards, procedures and guidelines

SEC Section L 'Smart Metering Key Infrastructure and DCC Key Infrastructure' does not contain any provisions for updated or replacement standards, procedures and guidelines in relation to the SMKI SEC Documents. Therefore, it is not explicitly clear who could define and provide a transitional period for Parties to move to a new or updated standard. Furthermore, when such standards, procedures and guidelines are updated, it is not clear who would update SEC related guidance to such documents.

Section G 'Security', specifically Sections G1.1-G1.4, includes provisions for updated or replacement standards, procedures and guidelines in relation to the security of the End-to-End Smart Metering System. These make it explicitly clear that the Security Sub-Committee (SSC), following delegation by the SEC Panel, is authorised to update any SEC related guidelines to these standards, as well as grant transitional periods when these standards are updated. This creates inconsistencies between Section G and Sections L as there are no such provisions for the SMKI PMA.

What is the impact this is having?

GPGs

If this issue is not addressed, the SEC will contain several references to GPGs that are no longer live or are subject to frequent change outside of SMKI PMA control. The latter could require frequent amendment to the SEC and to DCC Work Instructions if these references are left in the SEC. Furthermore, the existing references could be misleading for Parties that wish to access such guidance in the future.

Updated or replacement standards, procedures and guidelines

If this issue is not addressed, the SEC will contain ambiguity and inefficiencies for the SMKI PMA. Currently, it is not explicitly clear who is authorised to manage such standards, procedures and guidelines in relation to the SMKI Document Set. Also, the lack in provisions for transitional periods in relation to the SMKI SEC Documents could place unnecessary constraints on Parties trying to comply with these documents, since the GPGs will not be available for viewing.

3. Solution

Proposed Solution

Discontinued GPGs

Replacement SMKI PMA Guidance for GPGs

All references to GPGs 13, 43, 45 and 46 in the SEC will all be replaced with, 'SMKI PMA Guidance for [guidance title][2] published on the Website'.

'SMKI PMA Guidance' will be defined in Section A as;

- *means guidance in respect of the SMKI Document Set, updated from time to time by the SMKI PMA.*

Replacement SSC Guidance for GPGs

For GPG 18, the reference will be replaced with, 'Security Sub-Committee Guidance for [guidance title] published on the Website'.

'Security Sub-Committee Guidance' will be defined in Section A as;

- *means guidance in respect of the security of any System, updated from time to time by the Security Sub-Committee.*

The GPGs and the titles for each of the corresponding replacement guidance are outlined below:

GPG replacement guidance titles	
GPG ref.	**Title of replacement guidance**
GPG 13	Protective Monitoring
GPG 18	Forensic Readiness
GPG 43	Verifying Individual Identity
GPG 45	Verifying Individual Identity
GPG 46	Verifying Organisation Identity

These changes will minimise the risk of confusion. Furthermore, this would give clarity, including for GPG 13, that no further Draft Proposal is required if the SMKI PMA needs to change the guidance in the future. This is because the guidance will not sit within the SEC; instead it will be published as separate documents on the SECAS website.

Therefore, as part of this modification's implementation, SECAS and the SMKI Specialist will develop SMKI PMA guidance documents to publish and replace the individual GPGs for SMKI PMA review and approval. These guidance documents will be maintained and updated as necessary by the SMKI PMA without being subject to the Modifications Process, as they will not sit within the SEC.

---

[2] Each SMKI PMA or SSC Guidance will be individually titled in the SEC.

Updated or Replacement Standards, Procedures and Guidelines

Provisions will be placed in Section L1 'SMKI Policy Management Authority' that obligate the SMKI PMA to update standards, procedures and guidelines that apply to the operation of the SMKI Services and the DCCKI Service. These standards, procedures and guidelines will then be published on the SECAS website for efficiency and ease of access.

In addition, the SMKI PMA will determine the date from which the DCC or a User will be obligated to comply with any updated standards, procedures and guidelines. During the transitional period determined by the SMKI PMA, the DCC or the User will be obligated to comply (at its discretion) with:

- the previous version of the standard, procedure or guideline; or
- the updated or replaced standard, procedure or guideline.

The DCC or the User will be allowed to appeal any obligation date with the new or updated standards, procedures and guidelines to the SEC Panel.

Housekeeping changes

This modification will also make housekeeping changes to amend the typographical errors in the affected documents.

4. Impacts

This section summarises the impacts that would arise from the implementation of this modification.

SEC Parties

SEC Party Categories impacted			
✓	Large Suppliers	✓	Small Suppliers
✓	Electricity Network Operators	✓	Gas Network Operators
✓	Other SEC Parties	✓	DCC

The main impact is for the DCC who are required to operate the guidance. However, all Users who apply for SMKI Certificates could be affected by GPG 45 and GPG 46. This is since GPG 45 specifies the evidence required by the DCC to prove individual identity. In addition, GPG 46 specifies the evidence required for an Organisation to prove its identity when nominating a Senior Responsible Officer (SRO). SEC Parties who aren't applying for SMKI Certificates will be unaffected.

Only Other Users within the Other SEC Parties category will be impacted.

DCC System

This modification will not impact the DCC Systems.

SEC and subsidiary documents

The following parts of the SEC will be impacted:

- Section A 'Definitions and Interpretation'
- Section G 'Security'
- Section L 'Smart Metering Key Infrastructure and DCC Key Infrastructure'
- Appendix A 'Device Certificate Policy'
- Appendix B 'Organisation Certificate Policy'
- Appendix D 'SMKI Registration Authority Policies and Procedures'
- Appendix L 'SMKI Recovery Procedure'
- Appendix Q 'IKI Certificate Policy'

The changes to the SEC required to deliver the Proposed Solution can be found in Annex A.

Consumers

This modification will not have an impact on consumers.

Other industry Codes

This modification will not impact any other industry Codes.

Greenhouse gas emissions

This modification will not impact greenhouse gas emissions.

5. Costs

DCC costs

This modification will not incur any implementation costs on the DCC.

SECAS costs

The estimated SECAS implementation costs to implement this modification is four days of effort, amounting to approximately £2,400. The activities needed to be undertaken for this are:

- Updating the SEC and releasing the new version to the industry.
- Review and publication of the new SMKI PMA and SSC replacement guidance.

The SMKI PMA Chair and the SSC Chair have stated they will develop the new SMKI PMA and SSC replacement guidance. The guidance will be subsequently reviewed by each of the respective Sub-Committees.

SEC Party costs

This modification will not incur any implementation costs on SEC Parties.

6. Implementation approach

Approved implementation approach

The Panel has agreed an implementation date of:

- **5 November 2020** (November 2020 SEC Release) if a decision to approve is received on or before 22 October 2020; or
- **25 February 2021** (February 2021 SEC Release) if a decision to approve is received after 22 October 2020 but on or before 11 February 2021.

The SMKI PMA Chair and the Security Sub-Committee Chair will need to ensure that the replacement guidance is published on the SECAS website ahead of the recommended implementation date. SECAS will work with both the SMKI PMA and the SSC to achieve this.

7. Assessment of the proposal

Observations on the issue

The Change Sub-Committee (CSC) unanimously agreed that the issue is clearly defined and understood. It recommended that the Panel should covert this Draft Proposal into a Modification Proposal and, as it is a clear housekeeping change, that it should enter the Report Phase.

Solution development

SMKI PMA approach

Following on from the NCSC's response to the SECAS review, the SMKI PMA agreed that the GPG references in the SEC should be updated.

The SMKI PMA agreed to adopt bespoke guidance based on the GPGs and other available guidance, focussed on the smart metering context. It acknowledged that a modification would be needed to amend all the GPG references to e.g. "SMKI PMA Guidance published on the Website". This approach would minimise the potential for confusion. Furthermore, this would give clarity, including for GPG 13, that no further Draft Proposal is required if the SMKI PMA need to change the guidance in the future. Therefore, as part of this modification's implementation, SECAS and the SMKI Specialist will develop SMKI PMA guidance documents to publish and replace the individual GPGs for SMKI PMA review and approval. These guidance documents will be maintained and updated as necessary by the SMKI PMA without being subject to the Modifications Process, as they will not sit within the SEC.

Support for change

SMKI PMA

This proposal was raised on behalf of the SMKI PMA, who supports the proposed solution. It agreed that this change would give clarity to the SEC, as well as increase efficiency in reacting to changes to standards, procedures and guidelines.

Views against the General SEC Objectives

Proposer's views

Objective (b)[3]

The Proposer believes that MP115 could facilitate SEC Objective (b). The Proposed Solution will ensure the latest guidance on data protection and security is referenced in the SEC and made available to the DCC.

---

[3] Enable the DCC to comply at all times with the General Objectives of the DCC (as defined in the DCC Licence), and to efficiently discharge the other obligations imposed upon it by the DCC Licence.

Objective (f)[4]

The Proposer believes that MP115 will better facilitate SEC Objective (f). By removing the references to the outdated GPGs, the Proposed Solution will ensure Parties are provided with the most up-to-date guidance to ensure the protection of Data and the security of Data and Systems in the operation of this Code.

Objective (g)[5]

The Proposer believes that MP115 will better facilitate SEC Objective (g) by ensuring the Code is maintained in line with the SMKI PMA's and the SSC's updated and replacement guidance. This will be achieved by replacing the references to the GPGs with the relevant Sub-Committee's guidance. Furthermore, this will increase efficiency as any updates to the replacement guidance will not require a Draft Proposal in future.

---

[4] Ensure the protection of Data and the security of Data and Systems in the operation of this Code.

[5] Facilitate the efficient and transparent administration and implementation of this Code.

Appendix 1: Progression timetable

Timetable	
Action	**Date**
Draft Proposal raised	11 Feb 2020
Presented to CSC for final comment and recommendations	25 Feb 2020
Modification Report approved by Panel	13 Mar 2020
Modification Report Consultation	20 Apr 2020 – 11 May 2020
Change Board vote	27 May 2020

Appendix 2: Glossary

This table lists all the acronyms used in this document and the full term they are an abbreviation for.

Glossary	
Acronym	**Full term**
CESG	Communications-Electronics Security Group
CSC	Change Sub-Committee
CNI	Critical National Infrastructure
DCC	Data Communications Company
FIPS	Federal Information Processing Standards
GDS	Government Digital Service
GPG	Good Practice Guide
ISO	International Organization for Standardization
ISO/IEC	International Electrotechnical Commission
NCSC	National Cyber Security Centre
NIST	National Institute of Standards and Technology
RFC	Request for Comments
SEC	Smart Energy Code
SECAS	Smart Energy Code Administrator and Secretariat
SMKI PMA	Smart Metering Key Infrastructure Policy Management Authority
SRO	Senior Responsible Officer
SSC	Security Sub-Committee

MP115 'Changes to the NCSC Good Practice Guides'

Annex A

Legal text – version 1.0

About this document

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

Section A ‘Definitions and Interpretation’

These changes have been drafted against version 8.0 of Section A.

Add the following new definitions to Section A1 in alphabetical order:

Security Sub-Committee Guidance	means guidance in respect of the security of any System, updated from time to time by the Security Sub-Committee.
SMKI PMA Guidance	means guidance in respect of the SMKI Document Set, updated from time to time by the SMKI PMA.

Section G 'Security'

These changes have been drafted against version 8.0 of Section G.

Amend Sections 2.27 and 2.28 as follows:

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~~ 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.

~~(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.~~

Amend Section 8.6 as follows:

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

(a) employs consultants who are members of the Certified Cyber Professional (~~CPP~~CCP) scheme at the 'Lead' or 'Senior Practitioner' level in either the 'Security and Information Risk Advisor' or 'Information Assurance Auditor' roles; and

(b) engages those individuals as its lead auditors for the purposes of carrying out all security assurance assessments in accordance with this Section G8.

Section L 'Smart Metering Key Infrastructure and DCC Key Infrastructure'

These changes have been drafted against version 8.0 of Section L.

Add Sections 1.20, 1.21, 1.22 and 1.24 as follows:

Updated or Replacement Standards, Procedures and Guidelines

L1.20 In respect of the SMKI Document Set, the SMKI Services, the DCCKI Document Set, the DCCKI Services and Sections L2 to L13 shall be interpreted in accordance with the following provisions of this Section L1.

L1.21 As a consequence of its duties under Section L1.17, the SMKI PMA shall determine any updates that are required to standards, procedures and guidelines that apply to the operation of the SMKI Services and the DCCKI Services and shall publish the latest versions on the Website.

Transitional Period for Updated or Replacement Standards, Procedures and Guidelines

L1.22 Section L1.23 applies where:

(a) the DCC or any User is required, in accordance with any provision of the SMKI SEC Documents, 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.

L1.23 Where this Section L1.23 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 SMKI PMA 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.

L1.24 Any date determined by the SMKI PMA in accordance with Section L1.23 may be the subject of an appeal by the DCC or any User to the Panel (whose decision shall be final and binding for the purposes of this Code).

Amend Sections 9.9 and 9.15 as follows:

L9.9 For the purposes of the approval of the Device CPS by the SMKI PMA in accordance with Section L9.8(d):

(a) the DCC shall submit an initial draft of the Device CPS to the SMKI PMA by no later than the date which falls three months prior to the commencement of Systems Integration Testing or such later date as may be agreed by the SMKI PMA;

(b) the ~~SKMI~~ SMKI PMA shall review the initial draft of the Device CPS and shall:

  (i) approve the draft, which shall become the Device CPS; or

  (ii) state that it will approve the draft subject to the DCC first making such amendments to the document as it may direct; and

(c) the DCC shall make any amendments to the draft Device CPS that may be directed by the SMKI PMA, and the amended draft shall become the Device CPS.

L9.15 For the purposes of the approval of the Organisation CPS by the SMKI PMA in accordance with Section L9.14(d):

(a) the DCC shall submit an initial draft of the Organisation CPS to the SMKI PMA by no later than the date which falls three months prior to the commencement of Systems Integration Testing or such later date as may be agreed by the SMKI PMA;

(b) the ~~SKMI~~ SMKI PMA shall review the initial draft of the Organisation CPS and shall:

  (i) approve the draft, which shall become the Organisation CPS; or

  (ii) state that it will approve the draft subject to the DCC first making such amendments to the document as it may direct; and

(c) the DCC shall make any amendments to the draft Organisation CPS that may be directed by the SMKI PMA, and the amended draft shall become the Organisation CPS.

Appendix A 'Device Certificate Policy'

These changes have been drafted against version 1.0 of Appendix A.

Amend Sections 3.2.2 and 3.2.3 as follows:

3.2.2 Authentication of Organisation Identity

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

(i) procedure to be followed by a Party in order to become an Authorised Subscriber;

(ii) criteria in accordance with which the DCA will determine whether a Party is entitled to become an Authorised Subscriber; and

(iii) requirement that the Party shall be Authenticated by the DCA for that purpose.

(B) Provision is made in the SMKI RAPP for the purpose of ensuring that the criteria in accordance with which the DCA shall Authenticate a Party shall be set to the Level ~~3~~ pursuant to ~~GPG 46 (Organisation Identity, v1.0, October 2013), or to such equivalent level within a comparable authentication framework as may be agreed by the SMKI PMA~~ the SMKI PMA Guidance for Verifying Organisation Identity published on the Website.

3.2.3 Authentication of Individual Identity

(A) Provision is made in the SMKI RAPP in relation to the Authentication of persons engaged by Authorised Subscribers, which provides for all such persons to have their identity and authorisation verified to the Level ~~3 (Verified)~~ pursuant to the ~~CESG GPG43 RSDOPS framework, or to such equivalent level within a comparable authentication framework as may be agreed by the SMKI PMA~~ SMKI PMA Guidance for Verifying Individual Identity published on the Website.

Amend Section 4.1.3 as follows:

4.1.3 Enrolment Process for the Registration Authority and its Representatives

(A) Provision is made in the SMKI RAPP in relation to the establishment of an enrolment process in respect of DCA Personnel and DCA Systems:

(i) in order to Authenticate them and verify that they are authorised to act on behalf of the DCA in its capacity as the Registration Authority; and

(ii) including in particular, for that purpose, provision:

(a) for the face-to-face Authentication of all Registration Authority Personnel by a Registration Authority Manager; and

(b) for all Registration Authority Personnel to have their identify and authorisation verified to the Level ~~3 (Verified)~~ pursuant to the ~~CESG GPG43 RSDOPS framework, or to such equivalent level within a comparable authentication framework as may be agreed by the SMKI PMA~~ SMKI PMA Guidance for Verifying Individual Identity published on the Website.

Amend Section 5.1.1 as follows:

5 FACILITY, MANAGEMENT AND OPERATIONAL CONTROLS

5.1 PHYSICAL CONTROLS

5.1.1 Site Location and Construction

(A) The DCA shall ensure that the DCA Systems are operated in a sufficiently secure environment, which shall at least satisfy the requirements set out at Section G2 (System Security: Obligations on the DCC) and Section G5 (Information Security: Obligations on the DCC and Users) of the Code.

(B) The DCA shall ensure that:

(i) all of the physical locations in which the DCA Systems are situated, operated, routed or directly accessed are in the United Kingdom;

(ii) all bespoke Security Related Functionality is developed, specified, designed, built and tested only within the United Kingdom; and

(iii) all Security Related Functionality is integrated, configured, tested in situ, implemented, operated and maintained only within the United Kingdom.

(C) The DCA shall ensure that the DCA Systems cannot be indirectly accessed from any location outside the United Kingdom.

(D) The DCA shall ensure that the Device CPS incorporates provisions designed to ensure that all physical locations in which the manufacture of Certificates and Time-Stamping take place are at all times manually or electronically monitored for unauthorised intrusion in accordance with~~:~~ the SMKI PMA Guidance for Protective Monitoring published on the Website.

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

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

(E) The DCA shall ensure that the Device CPS incorporates provisions designed to ensure that all PINs, pass-phrases and passwords used for the purposes of carrying out the functions of the DCA are stored in secure containers accessible only to appropriately authorised individuals.

(F) The DCA shall ensure that the DCA Systems are Separated from any OCA Systems, save that any Systems used for the purposes of the Registration Authority functions of the DCA and OCA shall not require to be Separated.

Amend Section 5.4.2 as follows:

5.4.2 Frequency of Processing Log

(A) The DCA shall ensure that:

(i) the audit logging functionality in the DCA Systems is fully enabled at all times;

(ii) all DCA Systems activity recorded in the Audit Log is recorded in a standard format that is compliant with:

(a) British Standard BS 10008:2008 (Evidential Weight and Legal Admissibility of Electronic Information); or

(b) any equivalent to that British Standard which updates or replaces it from time to time; and

(iii) it monitors the DCA Systems in compliance with~~:~~ the SMKI PMA Guidance for Protective Monitoring published on the Website.

~~(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;~~

(B) The DCA shall ensure that the Device CPS incorporates provisions which specify:

(i) how regularly information recorded in the Audit Log is to be reviewed; and

(ii) what actions are to be taken by it in response to types of events recorded in the Audit Log.

(C) The DCA shall ensure that the Device CPS incorporates provisions in relation to access to the Audit Log, providing in particular that:

(i) Data contained in the Audit Log must not be accessible other than on a read-only basis; and

(ii) access to those Data must be limited to those members of DCA Personnel who are performing a dedicated system audit role.

SEC Appendix B ‘Organisation Certificate Policy’

These changes have been drafted against version 2.0 of Appendix B.

Amend Sections 3.2.2 and 3.2.3 as follows:

3.2.2 Authentication of Organisation Identity

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

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

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

(iii) requirement that the Party or RDP shall be Authenticated by the OCA for that purpose.

(B) Provision is made in the SMKI RAPP to ensure that each Eligible Subscriber has one or more DCC ID, User ID or RDP ID that is EUI-64 Compliant and has been allocated to that Eligible Subscriber in accordance with Section B2 (DCC, User and RDP Identifiers).

(C) Provision is made in the SMKI RAPP for the purpose of ensuring that the criteria in accordance with which the OCA shall Authenticate a Party or RDP shall be set to the Level ~~3~~ pursuant to ~~GPG 46 (Organisation Identity, v1.0, October 2013), or to such equivalent level within a comparable authentication framework as may be agreed by the SMKI PMA~~ the SMKI PMA Guidance on Verifying Organisation Identity published on the Website.

3.2.3 Authentication of Individual Identity

(A) Provision is made in the SMKI RAPP in relation to the Authentication of persons engaged by Authorised Subscribers, which provides for all such persons to have their identity and authorisation verified to the Level ~~3~~

~~(Verified)~~ pursuant to the ~~CESG GPG43 RSDOPS framework, or to such equivalent level within a comparable authentication framework as may be agreed by the SMKI PMA~~ SMKI PMA Guidance on Verifying Individual Identity published on the Website.

Amend Sections 4.1.2 and 4.1.3 as follows:

4.1.2 Enrolment Process and Responsibilities

(A) Provision is made, where applicable, in the SMKI RAPP in relation to the:

(i) establishment of an enrolment process in respect of organisations, individuals, Systems and Devices in order to Authenticate ~~-~~them and verify that they are authorised to act on behalf of an Authorised Subscriber or Eligible Subscriber in its capacity as such; and

(ii) maintenance by the OCA of a list of organisations, individuals, Systems and Devices enrolled in accordance with that process.

4.1.3 Enrolment Process for the Registration Authority and its Representatives

(A) Provision is made in the SMKI RAPP in relation to the establishment of an enrolment process in respect of OCA Personnel and OCA Systems:

(i) in order to Authenticate them and verify that they are authorised to act on behalf of the OCA in its capacity as the Registration Authority; and

(ii) including in particular, for that purpose, provision:

(a) for the face-to-face Authentication of all Registration Authority Personnel by a Registration Authority Manager; and

(b) for all Registration Authority Personnel to have their identify and authorisation verified to the Level ~~3 (Verified)~~ pursuant to the ~~CESG GPG43 RSDOPS framework, or to such equivalent level within a comparable authentication framework as may be agreed~~

~~by the SMKI PMA~~ SMKI PMA Guidance on Verifying Individual Identity published on the Website.

Amend Section 5.1.1 as follows:

5.1.1 Site Location and Construction

(A) The OCA shall ensure that the OCA Systems are operated in a sufficiently secure environment, which shall at least satisfy the requirements set out at Section G2 (System Security: Obligations on the DCC) and Section G5 (Information Security: Obligations on the DCC and Users) of the Code.

(B) The OCA shall ensure that:

(i) all of the physical locations in which the OCA Systems are situated, operated, routed or directly accessed are in the United Kingdom;

(ii) all bespoke Security Related Functionality is developed, specified, designed, built and tested only within the United Kingdom; and

(iii) all Security Related Functionality is integrated, configured, tested in situ, implemented, operated and maintained only within the United Kingdom.

(C) The OCA shall ensure that the OCA Systems cannot be indirectly accessed from any location outside the United Kingdom.

(D) The OCA shall ensure that the Organisation CPS incorporates provisions designed to ensure that all physical locations in which the manufacture of Certificates and Time-Stamping take place are at all times manually or electronically monitored for unauthorised intrusion in accordance with~~:~~ the SMKI PMA Guidance on Protective Monitoring published on the Website.

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

~~(ii) any equivalent to that CESG Good Practice Guide which updates or~~

~~replaces it from time to time.~~

(E) The OCA shall ensure that the Organisation CPS incorporates provisions designed to ensure that all PINs, pass-phrases and passwords used for the purposes of carrying out the functions of the OCA are stored in secure containers accessible only to appropriately authorised individuals.

(F) The OCA shall ensure that the OCA Systems are Separated from any DCA Systems, save that any Systems used for the purposes of the Registration Authority functions of the OCA and DCA shall not require to be Separated.

Amend Section 5.4.2 as follows:

5.4.2 Frequency of Processing Log

(A) The OCA shall ensure that:

(i) the audit logging functionality in the OCA Systems is fully enabled at all times;

(ii) all OCA Systems activity recorded in the Audit Log is recorded in a standard format that is compliant with:

(a) British Standard BS 10008:2008 (Evidential Weight and Legal Admissibility of Electronic Information); or

(b) any equivalent to that British Standard which updates or replaces it from time to time; and

(iii) it monitors the OCA Systems in compliance with~~:~~ the SMKI PMA Guidance on Protective Monitoring published on the Website.

~~(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;~~

(B) The OCA shall ensure that the Organisation CPS incorporates provisions which specify:

(i) how regularly information recorded in the Audit Log is to be reviewed; and

(ii) what actions are to be taken by it in response to types of events recorded in the Audit Log.

(C) The OCA shall ensure that the Organisation CPS incorporates provisions in relation to access to the Audit Log, providing in particular that:

(i) Data contained in the Audit Log must not be accessible other than on a read-only basis; and

(ii) access to those Data must be limited to those members of OCA Personnel who are performing a dedicated system audit role.

SEC Appendix D 'SMKI Registration Authority Policies and Procedures'

These changes have been drafted against version 2.0 of Appendix D.

Amend Sections 2 as follows:

2 SMKI Registration Authority obligations to support DCCKI identity verification

The DCCKI RAPP sets out the procedures by which nominated individuals may become DCCKI Senior Responsible Officers and/or DCCKI Authorised Responsible Officers in order to act on behalf of a Party, RDP or a DCC Service Provider in respect of DCCKI Services and DCCKI Repository Services. The DCCKI RAPP also sets out the activities undertaken by the DCC as DCCKI Registration Authority.

Upon request from the DCCKI Registration Authority to verify the identity of an individual nominated to be a DCCKI SRO or DCCKI ARO, the SMKI Registration Authority shall:

a) arrange a verification meeting with the nominated individual, at a date and time that is mutually agreed;

b) at the verification meeting, verify the individual identity of the nominated individual to the Level ~~3 (Verified)~~ pursuant to the ~~CESG GPG 45 (Identity Proofing and Verification of an Individual)~~ SMKI PMA Guidance on Verifying Individual Identity published on the Website, or except to the extent that the DCC otherwise notifies the SMKI Registration Authority, to such equivalent level within a comparable authentication framework as may be agreed by the SMKI PMA for the purposes of verification of individuals to become an SMKI SRO or SMKI ARO;

c) following the verification meeting, notify the nominated individual whether the process to verify their individual identity has been successful; and

d) following the verification meeting, confirm in writing to the DCCKI Registration Authority whether the identity of the individual has been successfully verified.

All other procedural steps required by which nominated individuals may become DCCKI Senior Responsible Officers and/or DCCKI Authorised Responsible Officers in order to act on behalf of a Party, RDP or DCC Service Provider (acting on behalf of the DCC) in respect of DCCKI Services and DCCKI Repository Services are as set out in the DCCKI RAPP.

Provided that the DCC need not repeat these processes in relation to an individual for the purposes of verifying their identity for the purposes of becoming a DCCKI SRO and/or DCCKI ARO where the required verification processes have already been carried out for the purposes of identifying them as being an SMKI SRO and/or SMKI ARO respectively.

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

Amend Table 5.1 as follows:

Step	When	Obligation	Responsibility	Next Step
5.1.8	In meeting to verify organisational identity	Verify: a) the organisational identity of the applicant organisation to the Level ~~3 (Verified)~~ pursuant to the ~~CESG GPG46 (Organisation Identity) , or to such equivalent level within a comparable authentication framework as may be agreed by the SMKI PMA~~ SMKI PMA Guidance on Verifying Organisation Identity published on the Website; b) via information held by SECCo, that the applicant organisation has the User Role or User Roles as specified in Organisation Information Form; c) proof of individual identity provided for the nominating individual against the information listed on the Organisation Information Form and the Nominee Details Form; and d) individual identity of the nominating individual to the Level ~~3 (Verified)~~ pursuant to the ~~CESG GPG45 (Identity Proofing and Verification of an Individual), or to such equivalent level within a comparable authentication framework as may be agreed by the SMKI PMA~~ SMKI PMA Guidance on Verifying Individual Identity published on the Website.	SMKI Registration Authority	If not successful, 5.1.9; if successful, 5.1.10

Amend Table 5.2 as follows:

Step	When	Obligation	Responsibility	Next Step
5.2.10	In SRO verification meeting	At the face-to-face SRO verification meeting, the SMKI Registration Authority shall, in person: a) check proof of individual identity provided for each nominated individual against the information listed on the SRO Nomination Form and the Nominee Details Form; and b) verify the individual identity for each nominated individual to the Level ~~3 (Verified)~~ pursuant to the ~~CESG GPG45 (Identity Proofing and Verification of an Individual), or to such equivalent level within a comparable authentication framework as may be agreed by SMKI PMA~~ SMKI PMA Guidance on Verifying Individual Identity published on the Website	SMKI Registration Authority	If not successfully verified, 5.2.11; if successfully verified, 5.2.12

Amend Table 5.3 as follows:

Step	When	Obligation	Responsibility	Next Step
5.3.10	In ARO verification meeting	At the ARO face-to-face verification meeting, the SMKI Registration Authority shall, in person, for the nominated individual: a) check proof of individual identity provided against the information listed on the ARO Nomination Form and Nominee Details Form; and b) verify the identity of the nominated individual to the Level ~~3 (Verified)~~ pursuant to the ~~CESG GPG45 (Identity Proofing and Verification of an Individual), or to such equivalent level within a comparable authentication framework as may be agreed by the SMKI PMA~~SMKI PMA Guidance on Verifying Individual Identity published on the Website	SMKI Registration Authority	If verified, 5.3.12; if not verified, 5.3.11

Amend Table 6.2 as follows:

Step	When	Obligation	Responsibility	Next Step
6.2.3	In verification meeting	The DCC shall, in accordance with the provisions of Sections G4.4 to G4.8: a) check proof of identity provided against the information provided by the nominated individual; and b) verify the identity of the nominated individual to the Level ~~3 (Verified)~~ pursuant to the ~~CESG GPG45 (Identity Proofing and Verification of an Individual), or to such equivalent level within a comparable authentication framework as may be agreed by the SMKI PMA~~SMKI PMA Guidance on Verifying Individual Identity published on the Website	DCC Chief Information Security Officer, on behalf of the DCC	If verified, 6.2.5. If not verified, 6.2.4

Amend Table 6.3 as follows:

Step	When	Obligation	Responsibility	Next Step
6.3.3	In verification meeting	In the verification meeting, the DCC shall, in accordance with the provisions of Sections G4.4 to G4.8: a) check proof of identity provided against the information provided by the nominated individual; and b) verify the identity of the nominated individual to the Level ~~3 (Verified)~~ pursuant to the ~~CESG GPG45 (Identity Proofing and Verification of an~~	SMKI Registration Authority Manager, on behalf of the SMKI Registration Authority	If successful, 6.3.5. If not successful, 6.3.4

Step	When	Obligation	Responsibility	Next Step
		~~Individual), or to such equivalent level within a comparable authentication framework as may be agreed by the SMKI PMA~~SMKI PMA Guidance on Verifying Individual Identity published on the Website		

SEC Appendix L ‘SMKI Recovery Procedure’

These changes have been drafted against version 2.0 of Appendix L.

Amend Table 3.4.3 as follows:

Step	When	Obligation	Responsibility	Next Step
3.4.3.8	At verification meeting	The DCC shall, in person, verify the individual identity of the nominated individual to the Level ~~3 (Verified)~~ pursuant to the ~~CESG GPG45 RSDOPS framework, or to such equivalent level within a comparable authentication framework as may be agreed by the SMKI PMA~~ SMKI PMA Guidance on Verifying Individual Identity published on the Website.	DCC	If successful for all, 3.4.3.10; for unsuccessful, 3.4.3.9

SEC Appendix Q ‘IKI Certificate Policy’

These changes have been drafted against version 2.0 of Appendix Q.

Amend Sections 3.2.2 and 3.2.3 as follows:

3.2.2 Authentication of Organisation Identity

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

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

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

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

(B) Provision is made in the SMKI RAPP for the purpose of ensuring that the criteria in accordance with which the ICA shall Authenticate a Party, RDP or SECCo shall be set to the Level ~~3~~ pursuant to ~~GPG 46 (Organisation Identity, v1.0, October 2013), or to such equivalent level within a comparable authentication framework as may be agreed by the SMKI PMA~~ the SMKI PMA Guidance on Verifying Organisation Identity published on the Website.

3.2.3 Authentication of Individual Identity

(A) Provision is made in the SMKI RAPP in relation to the Authentication of persons engaged by Authorised Subscribers, which provides for all such persons to have their identity and authorisation verified to the Level ~~3 (Verified)~~ pursuant to the ~~CESG GPG43 RSDOPS framework, or to such equivalent level within a comparable authentication framework as may be agreed by the SMKI PMA~~ SMKI PMA Guidance on Verifying Individual Identity published on the Website.

Amend Sections 4.1.2 and 4.1.3 as follows:

4.1.2 Enrolment Process and Responsibilities

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

(i) establishment of an enrolment process in respect of organisations, individuals and Systems in order to Authenticate them and verify that they are authorised to act on behalf of an Eligible Subscriber in its capacity as such; and

(ii) maintenance by the ICA of a list of organisations, individuals and Systems enrolled in accordance with that process.

4.1.3 Enrolment Process for the Registration Authority and its Representatives

(A) Provision is made in the SMKI RAPP in relation to the establishment of an enrolment process in respect of ICA Personnel and ICA Systems:

(i) in order to Authenticate -them and verify that they are authorised to act on behalf of the ICA in its capacity as the Registration Authority; and

(ii) including in particular, for that purpose, provision:

(a) for the face-to-face Authentication of all Registration Authority Personnel by a Registration Authority Manager; and

(b) for all Registration Authority Personnel to have their identify and authorisation verified to the Level ~~3 (Verified)~~ pursuant to the ~~CESG GPG43 RSDOPS framework, or to such equivalent level within a comparable authentication framework as may be agreed by the SMKI PMA~~ SMKI PMA Guidance on Verifying Individual Identity published on the Website.