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’

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.